نظرية التشفير والتعمية (الأساسيات)

الجزء الثاني

تأليف

د. ر. هانكرسون — د. غ. هوفمان

د. أ. لينورد — ك. ك. ليندنر

ك. ت. فيلبس — ك. أ. روجر

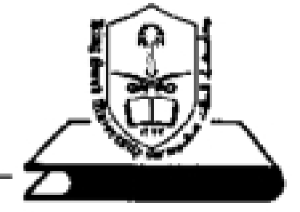
ج. ر. وول

ترجمة

د. معروف عبدالرحمن سمحان — د. فوزي بن أحمد الذكير

قسم الرياضيات - كلية العلوم

جامعة الملك سعود





النشر العلمي والمطابع - جامعة الملك سعود

ص.ب ٦٨٩٥٣ - الرياض ١١٥٣٧ - المملكة العربية السعودية

هذه ترجمة عربية مصرح بها من مركز الترجمة بالجامعة لكتاب:

Coding Theory and Cryptography: The Essentials
By: D. R. Hankerson, *et al*.

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

د. ر. هانكرسون

نظرية التشفير والتعمية: الأساسيات./ د. ر. هانكرسون؛ معروف عبدالرحمن سمحان؛ فوزي بن أحمد الذكير.- الرياض، ١٤٣٥هـ

٢مج

٢٣١ص؛ ١٧×٢٤سم

ردمك: ٥-٢١٧-٥٠٧-٦٠٣-٩٧٨ (مجموعة)

٩-٢١٩-٥٠٧-٦٠٣-٩٧٨ (ج٢)

١- الشيفرة ٢- الاختصارات ٣- أمن المعلومات أ. سمحان، معروف عبدالرحمن (مترجم) ب. الذكير، فوزي بن أحمد (مترجم) ج. العنوان

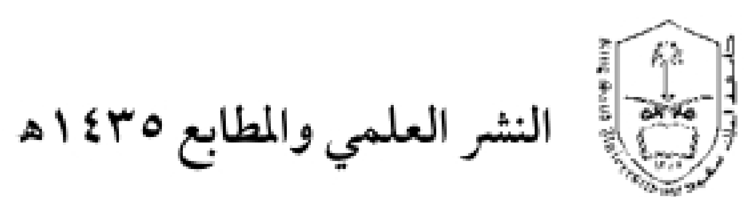
ديوي ٦٥٢,٨ ١٤٣٥/٩٨

رقم الإيداع: ٩٨/ ١٤٣٥

ردمك: ٥-٢١٧-٥٠٧-٦٠٣-٩٧٨ (مجموعة)

٩-٢١٩-٥٠٧-٦٠٣-٩٧٨ (ج٢)

حكمت هذا الكتاب لجنة متخصصة، وقد وافق المجلس العلمي على نشره في اجتماعه العشرين للعام الدراسي ١٤٣٣هـ/ ١٤٣٤هـ المعقود بتاريخ ١٦/ ٧/ ١٤٣٤هـ الموافق ٢٦/ ٥/ ٢٠١٣م.



النشر العلمي والمطابع ١٤٣٥هـ

مقدمة المترجمين

وقع اختيارنا على ترجمة هذا الكتاب لعدة أسباب أهمّها أن هذا الكتاب يجمع بين موضوعي نظرية التشفير ونظرية التعمية وهما الموضوعان اللّذان نقوم بتدريسهما في مقرر تطبيقات الجبر لطلاب قسم الرياضيات، ولذا فهو يخدم الهدف الذي نسعى إليه وهو توفير مادة علمية باللغة العربية لهذين الموضوعين لتكون في متناول الطالب. ومما يميز هذا الكتاب هو شرح مادة الرياضيات اللازمة لفهم المواضيع في المكان المناسب وبدون تعمق حيث يتطرق فقط إلى المفاهيم التي يحتاج إليها دون الخوض في براهين رياضية صعبة، وهذه الميزة تجعل هذا الكتاب مناسباً لطلبة الهندسة والحاسب الآلي بالإضافة إلى طلاب الرياضيات.

أثناء ترجمتنا لهذا الكتاب قمنا بتصحيح بعض الأخطاء المطبعية التي تمكنا من اكتشافها والتي لا يكاد يخلو منها أي كتاب. قمنا أيضاً بوضع بعض التفاصيل للمادة العلمية وأضفنا بعض البراهين التي نعتقد ضرورة وجودها وقد تم ذلك دون الإخلال بتسلسل المادة العلمية.

اعتمدنا في ترجمة المصطلحات العلمية على قاموس العلوم الرياضية الذي شارك المترجمان في إعداده والصادر عن منشورات جامعة الملك سعود وهو مبني على

المعجمين الصادرين عن مكتب تنسيق التعريب بالرباط ومعجم الرياضيات الصادر عن مؤسسة الكويت للتقدم العلمي ، واجتهدنا بترجمة المصطلحات التي لم ترد في أي من هذه المعاجم الثلاثة.

ونود أن نشكر مركز الترجمة بجامعة الملك سعود على موافقته على ترجمة هذا الكتاب الذي نأمل أن يكون إضافة مفيدة إلى المكتبة العربية. واللّه من وراء القصد.

المترجمان

إهداء المؤلفين

إلى زوجاتنا الحبيبات

سندي وجيل وجين وآن وجانيت وسو

إلى أولادنا

نويل وأيان وتيم وكيرت وجيمي وأندرو وميخان وكاترينا وريبركا

وإلى آبائنا وأمهاتنا

إيلين وريتشارد، ڤالي وجيل، مارجوري ولويس، ماري وتشارلز،

إيثل وريتشارد، أيريس وأيان، بيولاه ووالتر.

شكر وتقدير
Acknowledgments

نقدم شُكرنا العميق لألفريد مينيزس على اقتراحاته المفصّلة ومراجعاته العديدة للفصول من العاشر إلى الثاني عشر. كان من الممكن أن يحتوي هذا الكتاب على أخطاء أكثر وأن يكون سرد المادة أسوأ لولا ارشاداته الجمّة لنا. كما نود أن نقدم شُكرنا لسيلدا كيوسيكسفي على مراجعتها واقتراحاتها وتصحيحها لبعض الأخطاء. أما روزي توربرت فقد ساهمت مساهمة غير عادية بإنجاز أصول الطبعة الأولى من هذا الكتاب.

إن صبرها وشجاعتها على تحمل الأعباء الناتجة عن المراجعات الكثيرة يضعها في مصاف القديسين. كما نقدم شُكرنا وتقديرنا لهيذر كونر على العمل الرائع التي قامت به أثناء التحضير للطبعة الثانية. ونخص بالشكر مصممة الغلاف سندي أوترسون كما نقدر لها عملها معنا في العديد من المشاريع.

المؤلفون

تمهيد
Preface

الهدف من هذا الكتاب المنقّح والمحدّث من الطبعة الأولى هو تدريس نظرية التشفير والتعمية بأسلوب رياضي معقول لطلبة الهندسة وعلوم الحاسب والرياضيات. يختلف هذا الكتاب عن معظم كتب التشفير والتعمية الأخرى بنقطتين مهمتين هما "في الوقت المناسب" وإهمال التعميمات الرياضية غير المهمة.

إن فلسفة "في الوقت المناسب" مبنيّة على تقديم مادة الرياضيات اللازمة عند الحاجة إلى تطبيقها، ولذا، فالكتاب لا يحتوي على ٢٠٠ صفحة من الرياضيات (ليست ضرورة في معظمها) ومن ثم ٢٠٠ صفحة أخرى من التشفير والتعمية. وبهذا فإن شكل الكتاب هو على النحو التالي: رياضيات، تطبيقات، رياضيات، تطبيقات وهكذا. إن تجنب التعميمات الرياضية يعني على سبيل المثال، أنه ليس من الضروري وصف الشفرة الدورية على أنها مثالي رئيس. وبهذا فلقد أهملنا في العموم الخوض في التعميمات الرياضية والمفاهيم التي تستخدم عادة لتدريس المقرّر لطلاب الرياضيات فقط.

استخدم الجزء الأول من هذا الكتاب (الفصول من الأول إلى التاسع) لتدريس نظرية التشفير في فصلين متتاليين في جامعة أوبرن حيث كان المتطلب الوحيد أن يكون

لدى الطالب معلومات بدائية في الجبر الخطي. وبالطبع كلما كانت معلومات الطالب في الجبر الخطي والجبر المجرّد أكثر يكون استيعابه أفضل ومن ثم يحتاج إلى وقت أقصر لتغطية المادة الأوليّة.

يُركّز جزء نظرية التشفير من هذا الكتاب على إنشاء الشفرات الثنائية والشفرات على حقل مميزه 2، كما يُركّز على عمليتي التشفير وفك التشفير (تصويب الأخطاء) لعائلة من الشفرات المهمة. وعائلة الشفرات المختارة ذات أهمية خاصة للمهندسين ومتخصصي علوم الحاسب مثل شفرات ريد وسولومن وشفرات التلاف المستخدمة في اتصالات الفضاء وإلكترونيات المستهلك، ويعكس هذا الخيار المدى الواسع لخوارزميات التشفير وفك التشفير

أما الجزء الثاني من هذا الكتاب (الفصول من العاشر إلى الثاني عشر) فتبلورت فكرته بعد تدريسنا مقرراً بدائياً لفصل واحد في نظرية التعمية لطلاب جامعة أوبرن حيث الطلاب المسجلون في هذا المقرر هم خليط من طلاب مرحلة البكالوريوس وطلاب الدراسات العليا من تخصصات علوم الحاسب، الهندسة، الرياضيات، التربية حيث إن المعرفة الرياضية لبعضهم تقتصر على مقرر بدائي في الجبر أو نظرية الأعداد، ويعتبر ذلك كافياً لتقديم مقرر معقول في علم التعمية. في الحقيقة إن معظم المادة العلمية في هذا المقرر تحتاج فقط إلى النتائج الأساسية للأعداد الصحيحة قياس n (وهذه مقدمة في الفصل الحادي عشر). إن هدفنا الأساسي هو كتابة مقرر مختصر وتام لمقدمة في التعمية الحديثة مع التركيز على طرائق التعمية ذات المفتاح المعلن. في الفصل الثاني عشر قمنا بتغطية المواضيع الرئيسة في بنود قصيرة نسبياً وتركنا بعض الموضوعات للتمارين (تحتوي هذه التمارين على بعض التفاصيل والمراجع).

بوجه عام، نستطيع القول إن اهتمام نظرتي التعمية والتشفير هو نقل المعلومات إلكترونياً، مع مراعاة السريّة في الأولى والموثوقية في الثانية ومع اعترافنا بأن معظم الخطط الدراسية لا يتسع فيها المجال لتخصيص مقررات منفصلة لكل منها فإن هذا الكتاب يتيح تدريس الفصول من الأول إلى الرابع ومن ثم الفصلين الخامس والسادس أو الفصلين السابع والثامن لمقرر واحد في نظرية التشفير. من الممكن أيضاً تدريس الفصول من العاشر إلى الثاني عشر لمقرر في نظرية التعمية. كما أنه من الممكن تدريس الفصول الأول والثاني والثالث والعاشر والثاني عشر مع بعض موضوعات الفصل الحادي عشر لمقرر في التشفير والتعمية.

وأخيراً فالمؤلفون سيكونون ممتنين لأي ملحوظات يقدمها لهم مستخدمو هذا الكتاب على العنوان الإلكتروني: rodgec1@auburn.edu.

الرموز
Symbols

$C^{\perp}$: شفرة ثنوية للشفرة C .

C_{23} : شفرة جولاي.

C_{24} : شفرة جولاي الممتدة.

$GF(2^r)$: حقل جالوا.

$GF\left(2^r\right)[x]$: كثيرات حدود بمعاملات في الحقل $GF(2^r)$.

$RM(r,m)$: شفرة ريد ومولر.

$RS(2^r,\delta)$: شفرة ريد وسولومن.

S : الشفرة المولّدة بالمجموعة S .

المحتويات
Contents

الجزء الثاني: نظرية التعمية

الفصل العاشر

التعمية التقليدية
Classical Cryptography

التعمية هي عملية التواصل (نقل معلومات) بين طرفين مع وجود من يتنصت عليهم (أعداء)[1]. أهم الأمثلة على ذلك هو الحفاظ على سرية المعلومات أثناء التواصل باستخدام قناة اتصال غير آمنة. ويتم ذلك بقيام المرسل بتحريف محتوى الرسالة بحيث يكون من الصعب على من يعترضها من معرفة محتواها ولكن من السهل قراءتها من قبل المُسْتَقبِل (الصديق). وبهذا يمكن اعتبار عملية التعمية على أنها تقنية رياضية لحماية المعلومات (من الأعداء أو غير المصرح لهم معرفتها) وذلك بإجراء بعض التحويلات على هذه المعلومات.

إضافة إلى السرية، من الممكن استخدام التعمية لتحقق العديد من أهداف أمن المعلومات التي تعرف بالموثوقية (authentication) أو إثبات الأصالة التي تقدم لنا إثباتاً على التأكد من صواب مصدر الرسالة (أو أصل البيانات). أما سلامة البيانات (data integrity) فتكشف لنا التلاعب في البيانات من حيث تغييرها أو تأخير وصولها أو الرد غير الموثوق على الرسائل. ويكون دور المطابقة (identification) لإثبات التحقق من

---

(١) رايفست (Rivest)، انظر [71].

صحة هوية المستخدم. وعدم الإنكار (nonrepudiation) هي خدمة عدم السماح للمرسل التنصل (الإنكار) من أنه هو الذي قام بإرسال الرسالة. والتوقيع الإلكتروني (digital signature) هو رديف التوقيع الاعتيادي على الرسالة ويعد من أساسيات خطط الموثوقية.

تحليل التعمية (cryptanalysis) هو العملية العكسية للتعمية، وهي التقنية الرياضية المستخدمة لمحاولة كسر الرسالة المعماة ومن ثم قراءتها. تسمى عمليتي التعمية وتحليل التعمية بعلم التعمية (cryptology). يعد تحليل التعمية من العناصر المهمة لعلم التعمية التطبيقي حيث يلقى الضوء على مقدار ثقتنا بأمن خطة التعمية المستخدمة عند عدم وجود البرهان الرياضي على أمن هذه الخطة.

نقدم في البند (**١٠,١**) الإطار الأساسي المستخدم في الفصول العاشر والحادي عشر والثاني عشر. يعتمد أمن التواصل في التعمية التقليدية على سر يشترك فيه المتراسلون وندرس في البند (**١٠,٢**) بعض هذه الخطط التي تسمى خطط المفتاح المتماثل (symmetric-key schemes). إحدى هذه الخطط هي خطة اللفافة لمرة واحدة (one-time pad) وهي خطة بسيطة لا يمكن كسرها (آمنة تماماً) مهما كانت القدرة الحسابية التي يملكها العدو. ولكن هذه الخطة ليست عملية ويرجع السبب وراء ذلك لكبر المفتاح السري المستخدم. نناقش في البند (**١٠,٣**) نظام تعمية البيانات القياسي DES (Data Encryption Standard) وهو أفضل نظام تعمية متماثل المفتاح معروف لحد الآن. وعلى عكس الأمن التام لنظام اللفافة لمرة واحدة فقد صمم نظام DES لتكون كمية الحسابات اللازمة لكسره كبيرة جداً.

إحدى الخصائص الأساسية في أنظمة التعمية ذات المفتاح المتماثل هو معرفة المفتاح السري من قبل جميع المتراسلين حيث لا يمكن فصل القدرة على تعمية الرسالة عن القدرة على قراءتها. وفي العام ١٩٧٦م، نشر ديفي وهيلمان (Diffie and Hellman) (Diffie

بحثهما المشهور (انظر [27]) حيث اكتشفا نظام التعمية ذو المفتاح المعلن (public- key cryptography). حيث كانت أحد خصائصه هي الفصل بين مفتاح التعمية ومفتاح كسر التعمية ويعتمد أمن هذا النظام على صعوبة حل بعض المسائل الحسابية. نقدم في الفصل الحادي عشر بعض مواضيع نظرية الأعداد التي يعتمد عليها هذا النظام وفي الفصل الثاني عشر نقدم نظام التعمية ذو المفتاح المعلن وطرق تنفيذه.

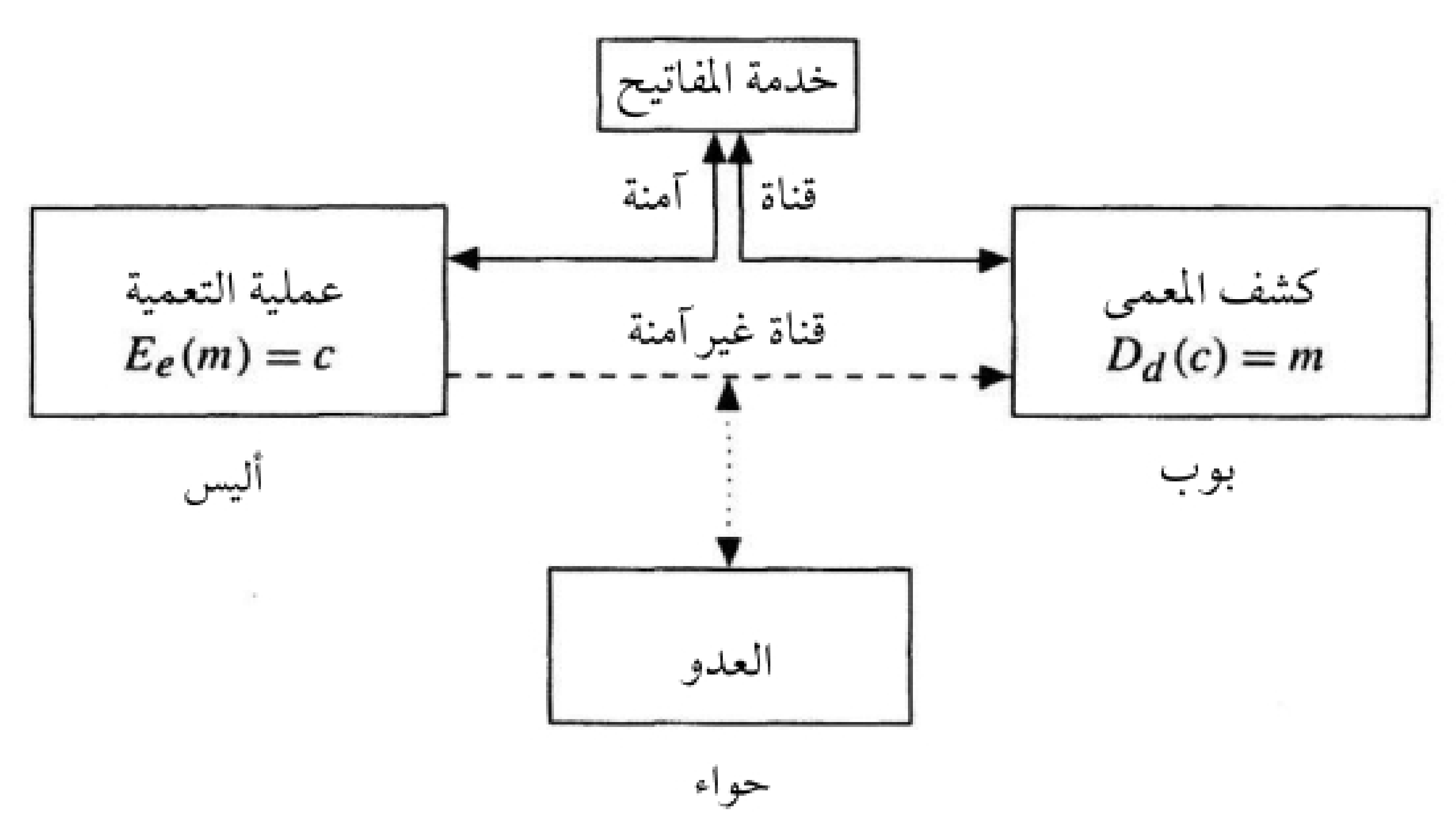
(١٠,١) خطط التعمية

Encryption Schemes

الهيكلية التالية هي التي نستخدمها عند دراسة أدوات عملية التعمية :

- هجائية منتهية $\mathcal{A}$.
- فضاء الرسائل $\mathcal{M}$ على $\mathcal{A}$ يتكون من كلمات رموز الهجائية. فعلى سبيل المثال، إذا كانت $\mathcal{A} = \{0,1\}$ فالرسائل هي عبارة عن كلمات تستخدم الرمزين 0 و 1. يرمز لمجموعة الرسائل من الطول n بالرمز $\{0,1\}^n$، كما أن $\{0,1\}^*$ هي مجموعة جميع الرسائل المنتهية الطول.
- تتكون خطة التعمية (أو التعمية) من فضائي رسائل $\mathcal{M}$ و $\mathcal{C}$ ومن مجموعة $\mathcal{K}$ (تسمى فضاء المفاتيح) ودالتين $E_k : \mathcal{M} \to \mathcal{C}$ و $D_k : \mathcal{C} \to \mathcal{M}$ لكل $k \in \mathcal{K}$ حيث $D_k\left(E_k(m)\right) = m$ لكل $m \in \mathcal{M}$. تسمى E_k دالة التعمية وتسمى D_k دالة كشف المعمى. كما تسمى عناصر $\mathcal{M}$، النص الواضح وعناصر $\mathcal{C}$، النص المعمى.
- تكتب المفاتيح في بعض خطط التعمية كأزواج مرتبة $k = (e,d)$ حيث يستخدم e في عملية التعمية و d في كشف المعمى. وفي هذه الحالة يسمى الزوج (e,d)، زوج مفتاح ونكتب $E_e = E_k$ و $D_d = D_k$.

يبين الشكل (١٠,١) **مخططاً** لعملية تعمية أساسية حيث تريد أليس (Alice) إرسال رسالة سرية m إلى بوب (Bob) مع محاولة حواء (Eve) وهي العدو، التنصت على قناة الإرسال غير الآمنة.



الشكل (١٠,١). التواصل باستخدام التعمية.

عند استخدامنا نظام تعمية متماثل المفاتيح (انظر البند (١٠,٢)) نحتاج إلى قناة آمنة لإرسال المفاتيح نفسها وهذا يتطلب أحياناً إلى وجود ناقل مفاتيح موثوق به أو أي طريقة آمنة أخرى للحفاظ على السرية. أما عند استخدامنا لأنظمة التعمية ذوات المفتاح المعلن (انظر الفصل الثاني عشر) فتزودنا القناة بطريقة للتحقق من موثوقية الجزء المعلن من المفتاح.

هناك نوعان من الأعداء، الأول منهما وهو العدو غير الفعال يقتصر عمله على التنصت على جزء من القنوات غير الآمنة ومحاولة معرفة جزء من معلومات الرسالة المرسلة من أليس إلى بوب. أما النوع الثاني فهو العدو الفعال حيث يحاول إضافة إلى التنصت، محاولة تحريف أو إرسال رسائل أو حتى قطع الإرسال تماماً بين

أليس وبوب. إن مهمة التعمية هي محاولة الحفاظ على أمن المعلومات واكتشاف الرسائل المحرفة والمزورة. ولهذا فعملية التعمية لا تضمن لنا عملية إرسال رسائل آمنة تماماً طالما هناك عدو فعال وأحياناً يتم إرسال رسائل بصفة دورية لمحاولة اكتشاف نقاط ضعف قنوات الاتصال.

من الممكن القول إن نظام التعمية يكون قابلاً للكسر (غير آمن) إذا استطاع العدو الحصول على النص الواضح من النص المعمى (والأسوأ من ذلك هو استطاعة العدو من حساب المفتاح السري للنظام). يمكن تقسيم أمن النظام إلى الأنواع التالية:

- يكون النظام آمن تماماً إذا كان من المستحيل معرفة النص الواضح من قبل العدو (ما عدا طول النص الواضح) مهما كان النص المعمى المتوفر لديه ومهما كانت مصادر الحسابات المتوفرة لديه.
- يكون النظام آمن حسابياً إذا كانت عملية كسره حسابياً غير ممكنة مع وجود مصادر معقولة للحسابات ومع استخدام التقنية المعروفة لتحليل النظام.
- يكون النظام آمن برهاناً إذا أمكن برهان أن كسره على الأقل يكافئ حل مسألة رياضية من المعلوم أنها صعبة الحل.

سنقدم في البنود القادمة بعض التفاصيل عن هذه الأنواع المتعلقة بأمن أنظمة التعمية.

وصف خان (Kahn) الكتاب الذي نشره كرتشوف (Kerchhoffs) في العام ١٨٨٣م بأنه ثاني أعظم كتب التعمية[٢]. احتوى كتاب كرتشوف على عدة شروط أساسية لاختيار نظام التعمية منها: يجب أن يكون النظام غير قابل للكسر (على الأقل من

(٢) ذكر خان (انظر Kahn [48]): يعود الفضل الأول لوضع خطة مترابطة منطقياً لفكرة علم التعمية إلى جيوڤاني باتيستا بورتا المولود في مدينة نابيلوس في بحثه المنشور عام ١٥٦٣م، ولكن هذه النظرة إلى التعمية لم تعد كافية بعد اكتشاف التيلغراف.

الناحية التطبيقية) إذا كان من غير الممكن أثبات أمنه رياضياً. لا يجب أن يؤثر التغاضي عن بعض خصائص النظام على عملية الإرسال. سهولة تذكر وتغيير مفتاح التعمية السري. إمكانية إرسال النص المعمى باستخدام التيلغراف. يجب أن يكون هناك مرونة في نقل أدوات ووثائق النظام وأن تكون قابلة للتنفيذ من قبل شخص واحد فقط ويجب أن يكون النظام سهلاً بحيث لا يحتاج إلى معرفة مسبقة لقواعد كثيرة ولا يحتاج إلى تفكير ذهني. وهذه الأخيرة تسمى أحياناً بقاعدة كرتشوف التي تنص على أن أمن النظام يجب أن يعتمد فقط على مفتاح التعمية. أي أنه يمكن المحافظة على أمن النظام حتى لو كان العدو على دراية بنظام التعمية المستخدم.

يكون هدف العدو أثناء عملية التعمية المبينة في الشكل (١٠,١) هو معرفة النص الواضح من النص المعمى أو معرفة المفتاح نفسه، وأحياناً يكون الهدف محدود بمعرفة نص واضح معين. وعند اعتراضه لبعض الرسائل المعماة يحاول دراسة أنماط الإرسال لمعرفة معلومات عن الرسالة. على سبيل المثال، يمكن ملاحظة التدفقات المفاجئة للمعلومات حتى مع عدم معرفة ماهية الرسالة. إن هدفنا هو محاولة كسر النظام نفسه وهناك عدة مستويات لذلك:

(١) معرفة النص المعمى فقط (cipher text-only attack). يحاول العدو هنا معرفة النص الواضح أو مفتاح التعمية من النص المعمى الذي بحوزته. يعدُّ النظام الذي يمكن كسره بهذه الطريقة غير آمن كلياً.

(٢) معرفة النص الواضح (known-plaintext attack). في هذه الطريقة يكون بحوزة العدو جزء من النص الواضح وما يقابله من النص المعمى. وفي هذه الحالة يحاول العدو معرفة المفتاح السري أو كشف تعمية نصوص معماة إضافية سبق وأن استخدمت المفتاح نفسه لتعميتها.

(٣) اختيار نص واضح (chosen-plaintext attack). في هذه الحالة يكون العدو قد استطاع الدخول مؤقتاً على أدوات التعمية (ليس المفتاح) ومن ثم أجرى عملية تعمية لبعض النصوص الواضحة. إذا تم اختيار النص المعمى بطريقة تعتمد على نتائج مسبقة فتسمى الطريقة بالهجوم التكيفي (adaptive attack).

(٤) اختيار نص معمى (chosen-ciphertext attack) في هذه الحالة يكون العدو قد استطاع الدخول مؤقتاً على أدوات التعمية ومن ثم يختار نصوص معماة ويجد ما يقابلها من النص الواضح.

هناك طرق أخرى لمحاولة كسر بعض الأنظمة التي تعتمد على خصائص أدوات التعمية، مثل ملاحظة الزمن اللازم للحسابات وغيرها (انظر [52] و [53]). وفي بعض الأحيان استخدمت الرشوة والابتزاز لمعرفة مفتاح التعمية.

(٢,١٠) التعمية ذات المفتاح المتماثل

Symmetric-Key Encryption

في عديد من أنظمة التعمية التقليدية يكون هناك كلمة سر (مفتاح) مشتركة بين المتراسلين وبمعرفة هذا السر يكون بإمكانهما التعمية وكشف المعمى. وبصورة أدق، نقول إن نظام التعمية متماثل المفتاح إذا كان إيجاد D_d من e و E_e من d يتطلب الوسائل نفسها.

يتكون نظام تعمية تعويض بسيط (Simple Substitution Cipher) من تطبيق آحادي k على الهجائية المستخدمة. تتم عملية التعمية بتطبيق k على كل من رموز الرسالة. أي إذا كان $m = m_0m_1 \dots$ حيث m_i رموز من الهجائية فإن:

$$E_k(m) = E_k(m_0m_1 \dots) = k(m_0)k(m_1)\dots$$

مثال (١٠،٢،١)

نظام الإزاحة (shift cipher) هو حالة خاصة من نظام التعويض. يكون المفتاح k ، $0 \le k \le n$ عبارة عن إزاحة ثابتة على رموز الهجائية $\{a_0, a_1, \dots, a_{n-1}\}$ حيث :

$$a_j \mapsto a_{(j+k) \bmod n}$$ [٣]

دالة التعمية المشهورة $\operatorname{rot}13$ تقابل $k = 13$ على الهجائية $\{a, b, \dots, z\}$ وذلك بالتدوير 13 موقعاً. أي أن الحروف تقابل الأعداد 0,1,...,25 وأن $\operatorname{rot}13$ تعني إضافة 13 إلى كل من حروف الهجائية ومن ثم نحسب الناتج قياس 26 [٤].

سنستخدم عادة الحروف الصغيرة للنص الواضح والحروف الكبيرة للنص المعمى. على سبيل المثال ،

$$\begin{aligned} \operatorname{rot}13(\text{rotate}) &= \operatorname{rot}13(17,14,19,0,19,4) \\ &= (4,1,6,13,6,17) \\ &= \text{EBGNGR} \end{aligned}$$

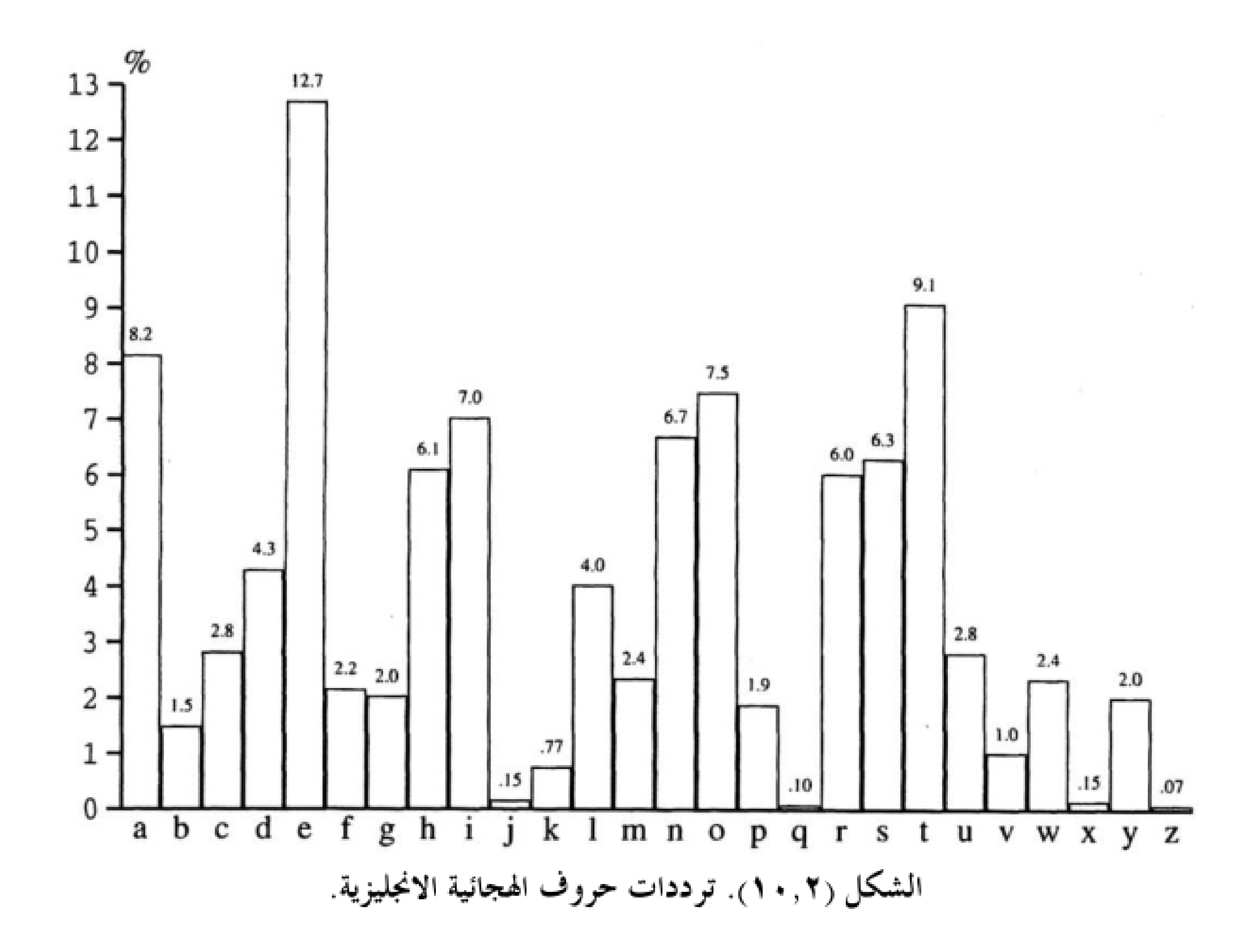
وبهذا فالنص الواضح "rotate" قد تمت تعميته إلى النص المعمى "EBGNGR". نظام الإزاحة هذا يحقق الخاصية $\operatorname{rot}13(\operatorname{rot}13(m)) = m$. أي أن دالة التعمية ودالة كسر التعمية هما الدالة نفسها. استخدم يوليوس قيصر (Julius Ceasar) نظام الإزاحة بمفتاح $k = 3$.

نظام الإزاحة غير آمن ويمكن كسره باستخدام طريقة اختيار النص الواضح. وهو غير آمن أيضاً باستخدام طريقة النص المعمى فقط ؛ لأن عدد المفاتيح هو 26 ومن الممكن تجريبها واحداً واحداً حتى نجد مفتاح التعمية. ▲

(٣) ندرس المفهوم " mod " في الفصل الحادي عشر وهنا يعني " $(i+k) \bmod n$ " باقي قسمة $i+k$ على n .

(٤) تستخدم $Rot13$ أحيانًا في USENET لتعمية العبارات التي تعتبر عدوانية.

قد يصعب كسر نظام تعمية تعويض بسيط باستخدام استنفاد المفاتيح حتى لو كان عدد رموز الهجائية صغيراً، ولكن يمكن كسره باستخدام تحليل التردد إذا كانت خواص الهجائية المستخدمة معروفة. على سبيل المثال، يبين الشكل (**١٠,٢**) ترددات حروف الهجائية الإنجليزية التي استندت إلى عينة مختارة من الصحف والروايات (انظر[3]). أي نص معمى لنظام تعمية تعويض بسيط يحقق توزيع ترددات الهجائية المستخدمة. فإذا كانت الهجائية المستخدمة هي الإنجليزية فنرى استناداً إلى الشكل (**١٠,٢**) أن الحرف الأكثر تردداً في النص المعمى يجب أن يقابل الحرف e (الأكثر تردداً في الهجائية الانجليزية) وأن ترددات الحروف $\{j,q,x,z\}$ صغيراً ومن ثم فإن ظهورها في النص المعمى نادر. من الممكن أيضاً الاعتماد على ترددات الثنائيات (حرفان متتاليان) والثلاثيات (ثلاثة حروف متتالية) بالأسلوب نفسه.



الشكل (١٠,٢). ترددات حروف الهجائية الانجليزية.

مثال (١٠,٢,٢)

لنفرض أن الهجائية هي الإنجليزية $\{a, b, \ldots, z\}$ وأن مفتاح نظام التعويض هو تبديلاً على الهجائية، على سبيل المثال،

$$k = \begin{pmatrix} a & b & c & d & e & f & g & h & i & j & k & l & m & n & o & p & q & r & s & t & u & v & w & x & y & z \\ T & U & V & W & X & Y & Z & B & I & K & E & A & C & D & F & G & H & J & L & M & N & O & P & Q & R & S \end{pmatrix}$$

حيث صور الصف الأول هي المقابلة لها في الصف الثاني، فمثلاً $E_k(\text{trek}) = \text{MJXE}$. من السهل تذكر هذا التبديل؛ لأن بداية الكلمة BIKE واقعة تحت الحرف h ومن ثم نملأ بقية الحروف بالترتيب. هذا النظام غير آمن ويمكن كسره باستخدام طريقة اختيار النص الواضح (من الممكن إيجاد المفتاح بتعمية الرسالة $m = abc \ldots z$). أما استخدام طريقة النص المعمى فقط لكسر النظام فتحتاج إلى بعض الجهد ولكنها تنجح في نهاية الأمر في كسر النظام. أما طريقة الاستنفاد لمعرفة مفتاح التعمية فهي مستحيلة؛ لأن عدد عناصر فضاء المفاتيح هو $26! \approx 4 \times 10^{26}$. ▲

يدعى نظام تعمية التعويض البسيط أحياناً بنظام تعمية التعويض الأحادي (monoalphabetic). إذا كانت الهجائية المستخدمة في نظام التعمية كبيرة فتصبح عملية تحليل (كسر) النظام باستخدام الترددات صعبة جداً. من الممكن إضافة رموز إضافية إلى هجائية صغيرة كالمستخدمة في المثال (**١٠,٢,٢**) لجعل فضاء الرسائل كبير ومن ثم يصعب كسره بتحليل الترددات. نظام البيانات القياسي DES (The Date Encryption Standard) الذي سندرسه في البند (**١٠,٣,٢**) هو عبارة عن نظام تعويض على هجائية سعتها 2^{64}.

الأنظمة التعددية

يمكن وصف الأنظمة التعددية على أنها أنظمة تحاول حجب ترددات المصدر الأصلي بحيث تُعمىَ كل من رموز النص الواضح إلى واحد من عدة رموز في النص المعمى. نظام فيجينير (Vigenere Cipher) هو مثال شائع على هذه الأنظمة. في هذا النظام يتم مقابلة رموز هجائية $\mathcal{A}$ مع الأعداد الصحيحة في الفترة $[0, |\mathcal{A}|]$ ومن ثم يتم اختيار

مفتاح $k = k_0k_1 \dots k_{n-1}$ حيث $k_i \in \mathcal{A}$. تتم عملية التعمية بتعمية قوالب من الهجائية طولها n ؛ وذلك بمقابلة رموز الرسالة مع رموز المفتاح قياس $|\mathcal{A}|$. على سبيل المثال، لنفرض أن $\mathcal{A}$ هي الهجائية الإنجليزية $\{a,b,\dots,z\}$ وتقابل مجموعة الأعداد $\{0,1,\dots,25\}$. الجدول التالي يوضح طريقة التعمية لنص واضح قصير باستخدام المفتاح "KEY".

النص الواضح	she sells sea shells by the seashore
المفتاح +	KEY KEYKE YKE YKEYKE YK EYK EYKEYKEY
النص المعمى	CLC C<u>IJVW</u> QOE QR<u>IJVW</u> ZI XFO WCKWFYVC

حيث عملية الجمع هي قياس 26. ويتم كشف المعمى بطرح كلمة المفتاح من النص المعمى قياس 26.

إن استخدام ترددات رموز المصدر (الهجائية) لكسر النظام التعددي أصعب قليلاً هنا ؛ وذلك لإمكانية تعمية رمز من النص الواضح إلى عدد من الرموز المختلفة في النص المعمى وهذا يعتمد على موقع الرمز، فمثلاً تمت تعمية الحرف "e" في المثال أعلاه إلى الحروف $\{C,I,O\}$. ومع ذلك، إذا استطعنا معرفة طول المفتاح l فمن الممكن استخدام تحليل الترددات لنظام أحادي على رسائل جزئية مكونة من الأحرف التي تكون المسافة بينها مضاعفات الطول l في النص المعمى. في المثال المقدم أعلاه، تتكون الرسائل الجزئية في النص المعمى من الأحرف في المواقع $0,3,6,\dots$ ويتم إنجاز ذلك بإضافة (قياس 26) الحرف الأول من الحروف الثلاثة لكلمة المفتاح إلى حروف النص الواضح في المواقع المقابلة.

اكتشف فردريك كاسيسكي (Friedrick Kasiski) في العام ١٨٦٣م طريقة تعرف الآن باسم اختبار كاسيسكي (Kasiski test) لمعرفة طول المفتاح بدراسة المسافات التي تفصل بين أجزاء متطابقة من النص المعمى(٥). في الغالب تقابل الكلمات المتطابقة في

(٥) كتب خان [48] أن كاسيسكي توفي في العام ١٨٨١م قبل أن يدرك تأثير الثورة التي سببها اكتشافه في علم التعمية.

النص الواضح الجزء نفسه من مفتاح التعمية مما ينتج عنه كلمات متطابقة في النص المعمى. في المثال السابق، يحدث ذلك في الجزء "ells" من النص الواضح. من الممكن وجود أجزاء متطابقة في النص المعمى لا تقابل أجزاء متطابقة من النص الواضح ولكن كلما زاد طول الرسالة كان احتمال ظهور مثل هذه الأجزاء صغيراً. ولهذا فعملية تطبيق اختبار كاسيسكي تبدأ في البحث عن كلمات مكررة في النص المعمى ونحسب المسافات بين هذه التكرارات فيكون طول كلمة السر هو أحد قواسم القاسم المشترك الأكبر لهذه الأطوال. لاحظ أن اختبار كاسيسكي يؤكد على أنه إذا وجدت كلمتان في النص الواضح بحيث يكون طول المسافة بينهما مضاعفاً لطول المفتاح فسيظهر هذا العدد كقيمة مسافة بين كلمتين متطابقتين في النص المعمى. هذا بالتأكيد ليس بالضرورة أن يكون صائباً دائماً ففي حالة الرسائل القصيرة يكون احتمال تطابق كلمتان في النص المعمى صغيراً على الأرجح. وأما في حالة الرسائل المعماة الطويلة جداً فمن الممكن حدوث ذلك لأسباب أخرى.

مثال (١٠,٢,٣)

تم استخدام نظام فيجينير لتعمية النص المعمى التالي حيث اللغة المستخدمة هي الانجليزية دون استعمال النقط والفواصل والفراغات. أي أن اللغة مكونة فقط من أحرف الهجائية $a, b, \ldots, z$ وعددها 26.

الأوفسيت	النص المعمى
0	UPVZB BVUPN KKFOL OGAKU FBTKF LFXUJ VIPZV KFZXO FIDLO ONLUP
50	KKFUZ OMQFQ MQXKU AFIUP VVVVK KFDFL DMFIU PVVFI ZVTMU XDBZY
100	FVVYF ZTHBA ZQHEY LTXVU JVXFM IDRSQ EJNCI PVZZQ HQEYJ BZQHB
150	YHTWL OUWND OLVUJ VREZA JHTWW VPTZW VLVDM TROPV XWIMN KJBVE
200	FITKV XRQEL FZOBY HSMND TVFOJ DZQHB YLOOZ QTQXK UISLS LNLUP
250	RESWB HOEZQ HERVC MRWJV XWIMR LSISR WMIHF TZQHN CXUBV UJVXF
300	JZTOJ VXGJA REMMU GPEEG PEEWP BYHXI KHS

الفراغات المبينة ليست ضمن النص المعمى ولكنها وضعت لتسهيل القراءة.

تظهر الكلمة من الطول 3 "ZQH" في عدد من المواقع حيث وضعنا خط تحت ثلاثة من هذه المواقع وهي 110 ، 138 ، 226 على التوالي. وبهذا من المرجح أن يقسم طول كلمة السر l الفرق بين أي عددين من هذه الأعداد، وهذه الفروقات هي:

$$226 - 110 = 2^2 \cdot 29 \qquad \text{و} \qquad 138 - 110 = 28 = 2^2 \cdot 7.$$

هذا يقترح علينا أن $l \mid \gcd\left(2^2 \cdot 7, 2^2 \cdot 29\right)$. أي أن $l \mid 2^2$. إذا كان $l = 1$ فيكون النظام هو نظام الإزاحة الأحادي.

في هذه المرحلة يقوم محلل التعمية بدراسة توزيع الترددات لكل من أطوال المفتاح المقترحة لمحاولة معرفة فيما إذا كان لها خواص الهجائية المستخدمة. الجدول التالي يبين هذه الترددات لكل من طولي المفتاح. فمثلاً، إذا كان $l = 2$ فالجدول يبين ترددات الرسائل الجزئية المكونة من رموز أوفسيت زوجية ومن ثم المكونة من رموز أوفسيت فردية. وهذا يعطينا:

ℓ	رسائل جزئية أوفسيت	ترددات أحرف الرسائل الجزئية (مرتبة تنازليًا)
2	$0, 2, 4, \ldots$	19 16 12 12 11 10 9 8 8 7 6 6 5 5 5 5 5 4 4 3 2 2 2 1 0 0
	$1, 3, 5, \ldots$	14 14 13 10 10 10 9 9 9 8 8 7 6 6 5 5 5 3 3 3 2 2 2 2 1 0
4	$0, 4, 8, \ldots$	12 10 10 7 6 6 6 5 5 4 2 2 2 1 1 1 1 1 1 1 0 0 0 0 0 0
	$1, 5, 9, \ldots$	10 9 8 7 5 5 5 5 5 5 4 3 3 2 2 2 1 1 1 0 0 0 0 0 0 0
	$2, 6, 10, \ldots$	12 11 8 8 7 5 5 5 4 4 2 2 2 2 2 1 1 1 1 0 0 0 0 0 0 0
	$3, 7, 11, \ldots$	9 9 8 8 7 5 5 5 4 3 3 3 3 3 2 2 2 1 1 0 0 0 0 0 0 0

من المتوقع أن يعكس كل سطر من السطور (في حالة الطول الصحيح للمفتاح) توزيع ترددات الهجائية المستخدمة. ومع أن الرسالة في هذا المثال قصيرة نسبياً إلا أنه يمكن ترجيح أن يكون طول المفتاح هو $l = 4$ وليس $l = 2$. وباستخدام توزيع الترددات المبينة في الشكل (**١٠,٢**) نجد أن الحرف "e" هو الأكثر تردداً في اللغة الانجليزية. وبهذا فمن الممكن أن يقابل أحد الحروف ذات الترددات العالية في النص المعمى (لكل صف من صفوف $l = 4$) "e". وفي هذا المثال من الممكن اختيار 3 أو 4 (أو

ربما أكثر من ذلك) من حروف النص المعمى (لكل صف من صفوف $l = 4$) لتقابل الحرف "e".

يبين الجدول التالي الحروف الأربعة الأكثر تردداً في كل من صفوف $l = 4$ وما يقابلها من حروف المفتاح (باعتبار أن كل من هذه الحروف تقابل الحرف "e").

حروف النص المعمى الأكثر ترددًا لصفوف $\ell = 4$		حروف المفتاح المقابلة
F J U P	$\xrightarrow{(c - e) \bmod 26}$	B F Q L
B V M I		X R I E
V Z R X		R V N T
K Q H L		G M D H

في هذه المرحلة يقوم محلل التعمية بكشف المعمى وذلك باستنفاد جميع كلمات المفتاح الممكنة والتي عددها في هذا المثال يساوي $256 = 4^4$.

في كثير من الأحيان يتم اختيار كلمة المفتاح من قاموس اللغة (أي أن المفتاح كلمة ذات معنى) مما يوفر على محلل التعمية الكثير من الجهد. ففي المثال أعلاه، يقود هذا البحث إلى الكلمتين "LEND" و "BIRD" وباستخدام الكلمة الثانية نرى أن النص الواضح هو:

النص المعمى	UPVZB BVUPN KKFOL OGAKU FBTKF LFXUJ VIPZV KFZXO FIDLO ONLUP
المفتاح	BIRDB IRDBI RDBIR DBIRD BIRDB IRDBI RDBIR DBIRD BIRDB IRDBI
النص الواضح	thewa terof thegu lfstr etche doutb efore hergl eamin gwith

والنص الواضح هو نص باللغة الإنجليزية ويكون كشف المعمى (بعد إعادة الفواصل والنقط) هو:

> The water of the Gulf stretched out before her, gleaming with the million lights of the sun. The voice of the sea is seductive, never ceasing, whispering, clamoring, murmuring, inviting the soul to wander in abysses of solitude. All along the white beach, up and down, there was no living thing in sight. A bird with a broken wing was beating the air above, reeling, fluttering, circling disabled down, down to the water.[٦]

(٦) من كتاب "اليقظة" لمؤلفته Kate Chopin.

تقابل كلمة النص المعمى "ZQH" التي استخدمناها في اختيار كاسيسكي لإيجاد طول المفتاح الكلمة الواضحة "ing". كان من الممكن استخدام كلمات أطول تكررت في النص المعمى، مثل "NLUP" و "ZQHBY" ويقابلان "with" و "ingth" حيث تكرر كل منها مرتان. لاحظ أيضاً أن الكلمة "PVZ" تكررت في الموقعين 1 و 135 وهذه تقابل "hew" و "mur" ومن ثم تعمدنا عدم استخدامها على اعتبار أن ذلك حدث مصادفة. هاتان الكلمتان يقترحان أن طول المفتاح يقسم 134 وهو ليس الطول الصحيح للمفتاح. ▲

يمكن إيجاد أمثلة أصعب على تحليل نظام فيجينير في كل من المرجعين [48] و [86] على وجه الخصوص نجد أن استخدام معامل الصدفة (index of coincidence) المعرف في المرجع [86] طريقة أفضل لإيجاد طول المفتاح وكلمة المفتاح.

نظام التعويض البسيط ونظام فيجينير هما مثالان على أنظمة التعمية القالبية (block ciphers) حيث يتم في هذه الأنظمة تحويل الرسالة باستخدام دالة ثابتة تؤثر في قوالب مكونة من عدد ثابت من الرموز. وهذه دوال عديمة الذاكرة، بمعنى أن الدالة المؤثرة على القالب لا تعتمد على موقع هذا القالب في الرسالة. وأما أنظمة السيل (stream ciphers) فهي على العكس من ذلك حيث الدالة المؤثرة على القالب تعتمد على موقع هذا القالب في الرسالة، ولهذا فأنظمة السيل تسمى أحياناً، أنظمة المرحلة (state ciphers).

تستخدم عادة الهجائية الثنائية $\mathcal{A} = \{0,1\}$ لتعريف مثل هذه الأنظمة حيث يعرف النظام القالبي (ونظام السيل) باستخدام عدد ثابت من البايتات تسمى طول القالب (block length). وتتم معالجة الرسائل على الهجائية $\mathcal{A} = \{a_0, \ldots, a_{n-1}\}$ بمقابلة $a_j \leftrightarrow j$ ثم تحويل j إلى كلمة ثنائية من الطول $\lceil \log_2 n \rceil$. في الحالة الخاصة التي يكون فيها عدد رموز الهجائية 26 (الهجائية الإنجليزية) كما هو مبين في المثال (**١٠,٢,٢**) نقوم باستبدال كل من رموز الهجائية بكلمة ثنائية طولها 5. على سبيل المثال،

$00110 = 6 \leftrightarrow g$. عندئذ، تؤثر دالتي التعمية وكشف المعمى في هذه الأمثلة على قوالب طول كل منها يساوي 5 .

إذا كانت m و m' رسالتين على $\{0,1\}$ من الطول نفسه فيكون $m \oplus m'$ هو الجمع قياس 2 ، على سبيل المثال، $0110 = 1010 \oplus 1100$. تسمى هذه العملية أحيانا بعملية الفصل المتنافية (exclusive or) وتكتب عادة XOR (عملية الجمع هذه تحقق حلم التلاميذ بإجراء عملية جمع دون الحاجة إلى حمل الأعداد للمرحلة التالية).

مثال (١٠,٢,٤)

نظام تعمية فيرنام (Vernam Cipher) هو نظام سيل على $\mathcal{A} = \{0,1\}$. وفضاء المفاتيح هو أيضاً كلمات على $A = \{0,1\}$. دالة التعمية هي $m \mapsto c = m \oplus k$. وبالحساب قياس 2 نستطيع الحصول على النص الواضح m من النص المعمى c على النحو التالي:

$$c \oplus k = m \oplus k \oplus k = m \oplus 0 = m$$

أي أن دالة كشف المعمى هي نفس دالة التعمية. ▲

إذا حصلنا على مراتب المفتاح (يسمى عادة مفتاح السيل) من محاولات بيرنولي المستقلة باحتمال $\frac{1}{2}$ (مثل، الرميات المستقلة لقطعة نقود غير منحازة) وإذا استخدم المفتاح مرة واحدة فقط فنحصل على نظام تعمية اللفافة الواحدة (one-time pad) وهو نظام آمن تماماً ضد محاولة كسره بمعرفة النص المعمى فقط. يرجع سبب أمن هذا النظام إلى أن طول مفتاح التعمية يساوي طول النص الواضح (ومن ثم طول النص المعمى) ويستخدم لمرة واحدة فقط. استخدم شانون (Shannon) في العام ١٩٤٠م [80] مفهوم الانتروبيا (entropy) لإثبات الأمن التام لنظام تعمية اللفافة الواحدة حيث برهن أن أي نظام تعمية متماثل المفاتيح يعد آمن تماماً طالما كان طول المفتاح مساوياً لطول الرسالة.

في بداية اكتشاف نظام فيرنام كانت معلومات المفتاح تكتب على ورقة (لفافة) ثم تتلف هذه اللفافة بعد كل عملية تعمية ومن هنا جاءت التسمية "اللفافة الواحدة". لاحظ أن استخدام المفتاح نفسه لتعمية أكثر من رسالة واحدة يؤدي إلى ضعف أمن النظام، على سبيل المثال، إذا كان $c = m \oplus k$ و $c' = m' \oplus k$ فنرى أن:

$$c \oplus c' = \left(m \oplus k\right) \oplus \left(m' \oplus k\right) = m \oplus m'$$

(على وجه الخصوص إذا كان $m = m'$ فيستطيع محلل التعمية اكتشاف ذلك بسهولة).

جرت عدة محاولات من قبل محللي التعمية لكسر النظام؛ وذلك بالحصول على بعض المفاتيح والاحتفاظ بها حيث صرح ضابط المخابرات البريطانية، بيتر رايت (Peter Wright) (انظر [101]) أن تكرار الاتحاد السوفيتي لاستخدام مفتاح تعمية في أكثر من عملية تعمية واحدة (قام بإرسال اللفافة نفسها إلى عديد من سفاراته في الغرب أثناء الحرب العالمية الثانية) أدى إلى كسر نظام اللفافة الواحدة حيث قام محللو التعمية المعروفة باسم VENONA من اختبار عديد من الرسائل المعمية ومقارنتها مع الرسائل المرسلة من الاتحاد السوفياتي عبر قنوات مختلفة(٧).

يتنازل نظام DES المشهور عن استخدام اللفافة الواحدة ويستخدم خطط تعمية أكثر مرونة يعتقد أنها آمنة حسابياً حيث توجد طرق شائعة لتوليد المفاتيح عشوائياً. تولّد هذه الطرق متتالية من الأعداد يتم تحديدها تماماً بمعرفة بذرة بدائية (initial seed)

---

(٧) قدمت محطة CNN التلفزيونية مسلسلاً عام ١٩٩٨م "خبرة الحرب الباردة" وكجزء من هذا المسلسل ذكرت أن مجموعة VENONA التابعة لهيئة USNSA تمكنت من كسر العديد من أنظمة التعمية (ومن ضمنها نظام تعمية اللفافة الواحدة) التي استخدمها الاتحاد السوفياتي خلال الفترة من ١٩٤٣م إلى ١٩٨٠م حيث تم الكشف عن هذه المصادر السرية في العام ١٩٩٥م. ولكن محطة CNN تجاهلت حقيقة استخدام المفتاح أكثر من مرة واحدة، الأمر الذي أخل لأمن النظام وادعت أن نظام اللفافة الواحدة قابل للكسر بتجريب عدة ملايين من الرسائل المعماة.

يتم اختيارها من مجموعة منتهية. وعلى الرغم من أن هذه المتتاليات لها العديد من الخصائص اللازمة للمحاكاة إلا أنها ليست عشوائية بالمعنى المطلوب في عملية التعمية[٨].

تمارين

(**١٠,٢,٥**) استخدم نظام فيجينير المبين في المثال (**١٠,٢,٣**) للحصول على النص المعمى التالي:

النص المعمى	العداد
VHVVG NRWGA EGCLJ RVHVO GAUHT OWWJE FSROJ LVIFQ KNKKG IIDPG	0
VUJAM HLUJW CLCRY EUWJE DVGLM HUBFW JTFEG CFPGV LOPEI DDLVW	50
QOLUE ALVGM VVJAC OCTKD EKKKG MRVBE BHRLR QPEUW QMFUT ONLPD	100
RBNIX KVBLM	150

جد مفتاح التعمية إذا علمت أن الكلمات من الطول 3 التي تحتها خط تقابل كلمة طولها 3 شائعة الاستخدام و أن الحرفين AE هما الحرفان an التي تبدأ بهما كلمة طولها 3.

(**١٠,٢,٦**) اكتب برنامجاً لتنفيذ نظام تعويض مماثل للمقدم في المثال (**١٠,٢,٢**) (استخدم المؤلفون المفتاح awk). يجب أن يقبل البرنامج كلمة المفتاح والصفوف على أنها مدخلات. بعد ذلك اختار نص واضح من اللغة الانجليزية طوله على الأقل 300 حرف ثم استخدم البرنامج للحصول على النص المعمى المقابل وبعد ذلك استخدم تردد اللغة لكسر النظام على اعتبار عدم معرفتك لكلمة المفتاح.

(**١٠,٢,٧**) هذا التمرين مخصص لكسر نظام فيجينير بالأسلوب المتبع في المثال (**١٠,٢,٣**) حيث نقدم معلومات كافية لمعرفة مفتاح التعمية ومن ثم النص الواضح

---

(٨) اكتشف جولدبيرج (Goldberg) وواجنر (Wagner) (انظر [39]) أن مولد الأعداد العشوائية المستخدم في تصفح الشبكة العنكبوتية Netscape أضعف مما ادعى مالك الموقع وهذا يؤدي إلى عدم ضمان أمن الصفقات التجارية وتسبب ذلك في الإحراج لمالك الموقع حيث منع الجمهور من استخدام خوارزميات أمن النظام.

دون استخدام الحاسب الآلي. ونترك خيار مثال أكثر واقعية للقارىء الذي يملك برنامج آلي لكسر النظام. استخدم نظام فيجينير للحصول على النص المعمى التالي :

العداد	النص المعمى
0	TUIRD SFOGK YLBVL OORXX RVDPL SHRSB POCBT TLQPG AOMHM SVONM
50	HDHDN TRTCX RYCJL NHGHT BRIIM HHQWB NHGTI ERDAX BHWCZ IQGEB
100	RHRQR TKSGX VRZJM IRBXG BXQWT RHGIU ELXXG GDIIA OUWIB EVAPR
150	DHQXW EWCTQ THBSF AUHXT LOOLN NWWAM HHOHB AQUPF EVGRA EGIAX
200	DICGL ESHTF BHFGX MRJXG GPOGM IDZAT WZCJE DESPL IJBPE AGWEE
250	OPOIL ALREX OSZTP OXZSM ANSXM TRATT NWVPM WKOIA ASDTG EGPTY
300	OUSRH UORHM AUHJI AJOXG IQOHM AWSRH UQQXE MHSIB NJCCP EGBTL
350	DDMBK LLRTY EQRTW BHWYB NJGJL ERTBB LLHPK YICGV EWCRK AFYSH
400	WQCCM HHGIN DHBIF OYSBX NWHWX CUIHA IQUDY TKSRH UQHTK RHJDE

الكلمة المكررة "MHH" تقع في المواقع 74 ، 179 ، 404 (خيارات أخرى ممكنة مثل الكلمة الأطول "SRHU").

(أ) إذا كان l هو طول كلمة المفتاح (غير المعلومة) فيمكن توقع أن $l \mid \left(179-74\right)=3\cdot5\cdot7$ وأن $l \mid \left(404-179\right)=3^2\cdot5^2$. إذا افترضنا أن هذه الكلمات المكررة من النص المعمى تقابل أجزاء متطابقة من النص الواضح فأثبت أن $l\in\left\{1,3,5,15\right\}$.

(ب) لنفرض أن l لا يمكن أن يكون 15.

الجدول التالي يبين ترددات أحرف النص المعمى (عددها 830) لبقية قيم l :

فسر لماذا يكون $l=5$ هو طول المفتاح المرجح.

(ج) جد حرف المفتاح المقابل لعدة أحرف كثيرة التردد في النص المعمى في الحالة $l=5$ على اعتبار أن هذه الأحرف تقابل الحرف e من النص الواضح.

(د) إذا افترضنا أن واضع التعمية اختار كلمة المفتاح من القاموس (أي كلمة ذات معنى) فجد كلمة المفتاح ، ثم جد جزء من النص الواضح. لاحظ أن بعض الرسائل الجزئية تحتوي على حروف ترددها كبير.

ℓ	العداد	ترددات حروف الرسائل																									
1	0, 1, …	60	53	45	42	40	40	39	39	39	39	38	37	33	32	30	27	27	26	25	25	21	20	17	13	13	10
		H	T	R	E	O	W	B	D	G	I	S	A	X	L	Q	C	P	U	M	N	F	V	K	J	Y	Z
3	0, 3, …	22	19	18	18	16	14	13	13	13	13	13	11	11	9	9	9	8	8	8	8	6	5	5	4	3	1
		H	E	B	R	T	O	A	G	I	S	W	C	U	D	Q	X	F	L	N	P	M	K	V	Z	J	Y
	1, 4, …	22	17	16	15	15	14	14	13	13	11	11	10	10	10	9	9	9	9	8	8	8	7	6	6	4	3
		H	T	G	D	W	O	X	A	E	Q	R	I	K	S	B	C	N	V	L	P	U	M	J	Y	F	Z
	2, 5, …	20	16	16	16	16	15	15	12	12	12	12	11	11	10	10	10	10	9	8	7	7	6	6	4	3	2
		T	H	I	L	R	D	S	B	M	O	W	A	P	E	G	Q	X	F	N	C	U	V	Y	J	Z	K
5	0, 5, …	24	15	15	13	12	12	11	11	7	7	6	5	5	4	4	3	3	3	3	2	1	0	0	0	0	0
		E	A	N	T	O	R	I	S	B	D	U	H	L	C	G	M	P	W	Y	V	F	J	K	Q	X	Z
	1, 6, …	22	15	14	14	13	12	12	10	8	8	6	6	6	5	4	3	2	2	1	1	1	1	0	0	0	0
		H	Q	D	U	W	L	R	O	K	V	F	G	J	P	X	S	I	Y	B	E	N	Z	A	C	M	T
	2, 7, …	18	15	13	13	12	11	9	9	9	8	7	7	6	5	5	4	3	3	2	2	2	2	1	0	0	0
		S	O	H	W	Q	C	G	I	R	B	A	F	Z	D	V	M	T	U	J	P	X	Y	K	E	L	N
	3, 8, …	24	14	13	12	12	11	11	10	9	8	7	7	6	6	5	2	2	2	2	2	1	0	0	0	0	0
		T	P	I	C	X	D	H	G	A	E	R	W	B	S	J	L	N	Q	V	Y	U	F	K	M	O	Z
	4, 9, …	18	17	15	13	13	10	9	9	8	7	7	6	5	4	4	4	3	3	3	3	2	2	1	0	0	0
		M	B	X	L	T	G	E	H	K	F	N	A	R	I	W	Y	O	P	V	Z	D	U	Q	C	J	S

(١٠,٢,٨) تؤدي عملية ضغط البيانات إلى إزالة بعض البيانات الزائدة. إذا استخدمنا عملية ضغط البيانات ثم عملية التعمية فهل يؤدي ذلك إلى نظام أكثر أمناً ؟

(١٠,٣) أنظمة تعمية فيستل و DES

Feistel Ciphers and DES

ندرس في هذا البند بصورة مختصرة صنف من أنظمة التعمية يتضمن نظام المفتاح المتماثل الأكثر شهرة وهو نظام DES. يتركز اهتمامنا هنا على بناء هذه الأنظمة وأمنها وعلى القارئ المهتم بتفاصيل نظام DES الرجوع إلى المراجع المقدمة في البند (١٠,٤).

نقدم هنا نظامي تعمية هما نظام البيانات الجديد المحكم (New Date Seal) أو اختصارا DES ونظام تعمية البيانات القياسي (Date Encryption Standard) أو اختصاراً DES حيث يعتمد بناء كل منهما على نظام فيستل. أنظمة فيستل هي أنظمة قالبية ينبثق عنها أنظمة مثل DES تستخدم أساليب بناء بحيث يمكن اعتبار خطة التعمية على أنها

خطة نظام سيل . إن أهم شروط بناء أنظمة التعمية القالبية هو سعة فضاء المفاتيح التي يفترض أن تكون كبيرة ليستعصي على محلل التعمية كسر النظام (معرفة المفتاح) بطريقة الاستنفاد. كما يشترط أن يكون طول القالب كبيراً لكي يجعل عملية تجميع بيانات من النص المعمى لتخمين المفتاح أمراً صعباً جداً. يكون هدف التشويش (confusion) هو تعقيد العلاقة بين المفتاح والنص المعمى وأما هدف النشر (diffusion) فهو محاولة نشر النص المعمى بحيث يعتمد حرف من حروف النص المعمى على عدد كبير من حروف النص الواضح. كما يتطلب بناء نظام تعمية عدم تجاهل سرعة وسعة ذاكرة الجهاز المستخدم لتنفيذ عملية التعمية.

يكون طول النص المعمى في نظام فيستل مساوياً لطول رسائل النص الواضح وليكن $2n$ حيث $n \in \mathrm{N}$. مدخل الخطة هو الرسالة نفسها والمفتاح k ويتم تنفيذ خوارزمية التعمية بسلسلة من المراحل عددها r .

- خوارزمية جدولة المفاتيح حيث يتم توليد مفاتيح جزئية $k_1, k_2, \dots, k_r$ من مفتاح معطى k . كل من هذه المفاتيح الجزئية تعرف دالة :

$$f_{k_i} : \{0,1\}^n \to \{0,1\}^n$$

- تقسم الرسالة m من الطول $2n$ إلى قسمين أيسر وأيمن وتكتب $m = (m_0, m_1)$. ويتم كتابة المراحل على النحو التالي :

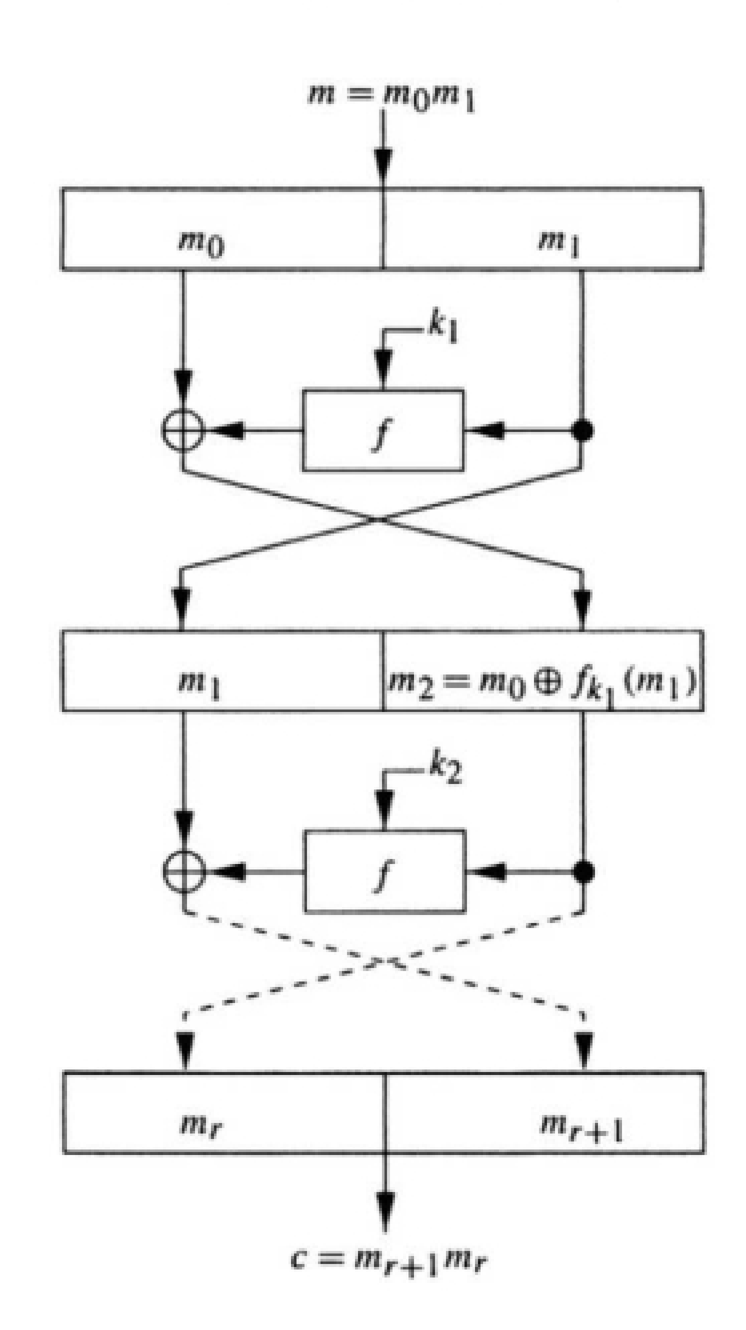
$$\begin{aligned} 1 &: (m_0, m_1) \mapsto (m_1, m_2 = m_0 \oplus f_{k_1}(m_1)) \\ 2 &: (m_1, m_2) \mapsto (m_2, m_3 = m_1 \oplus f_{k_2}(m_2)) \\ &\vdots \qquad\qquad\qquad \vdots \\ r &: (m_{r-1}, m_r) \mapsto (m_r, m_{r+1} = m_{r-1} \oplus f_{k_r}(m_r)) \end{aligned}$$

يقوم المخرج بتبديل النصف الأيمن مع النصف الأيسر للمرحلة الأخيرة لنحصل على $c = (m_{r+1}, m_r)$.

- إن هذا التبديل يسهل عملية كشف المعمى بحيث يسمح باستخدام المراحل r نفسها (نفس الترتيب) وبعكس ترتيب المفاتيح الجزئية. ولرؤية ذلك، بوضع $c_j = m_{r+1-j}$ نرى أن $c = (c_0, c_1)$ ويمكن إيجاد m_{r-1} من المراحل لنحصل على:

$$c_2 = m_{r-1} = m_{r+1} \oplus f_{k_r}(m_r) = c_0 \oplus f_{k_r}(c_1)$$

وهذا هو الشكل الذي نحصل عليه من المرحلة 1.



سلم فيستل ملتو

إن استخدام المراحل على هذه الصورة يسمح لنا باستخدام دالة بسيطة عند كل مرحلة. وعند استخدام مراحل متعددة (يستخدم DES عدد $r = 16$ من المراحل) نستطيع إدخال تشويش ونشر. ومن الضروري أن تكون سعة فضاء المفاتيح كبيرة لتمنع

العدو من إمكانية الحصول على المفتاح بطريقة الاستنفاد على اعتبار أن لديه أدوات حسابية سريعة.

(١٠,٣,١) نظام البيانات الجديد المحكم

نظام NDS من أنظمة فيستل البسيطة ؛ وذلك لأن جدول المفاتيح يتكون من مفتاح واحد فقط. ولذا فهو سهل الكسر بطريقة اختيار النص الواضح كما سنرى في هذا البند.

ندرس هنا الحالة التي يكون فيها $n = 64$ (وبهذا يكون طول الرسائل هو $2n = 128$ مرتبة) وعدد المراحل هو $r = 16$. المفتاح هو الدالة $k : \{0,1\}^8 \to \{0,1\}^8$. من الواضح أن الشرط اللازم (وليس الكافي) على طول المفتاح لكي يمنع كسر النظام بطريقة استنفاد المفاتيح محققاً ؛ لأن طول المفتاح هو $2^{2048} = \left(2^8\right)^{2^8}$ وهذا عدد كبير جداً.

يحتوي النظام على دالتين (غير سريتين) $S_0, S_1 : \{0,1\}^4 \to \{0,1\}^4$ ويتكون جدول المفاتيح من المفتاح الوحيد k المستخدم في كل مرحلة من مراحل التعمية. لحساب $f_k\left(m_i\right)$ لنصف رسالة m_i من الطول 64 نقوم بتنفيذ التالي :

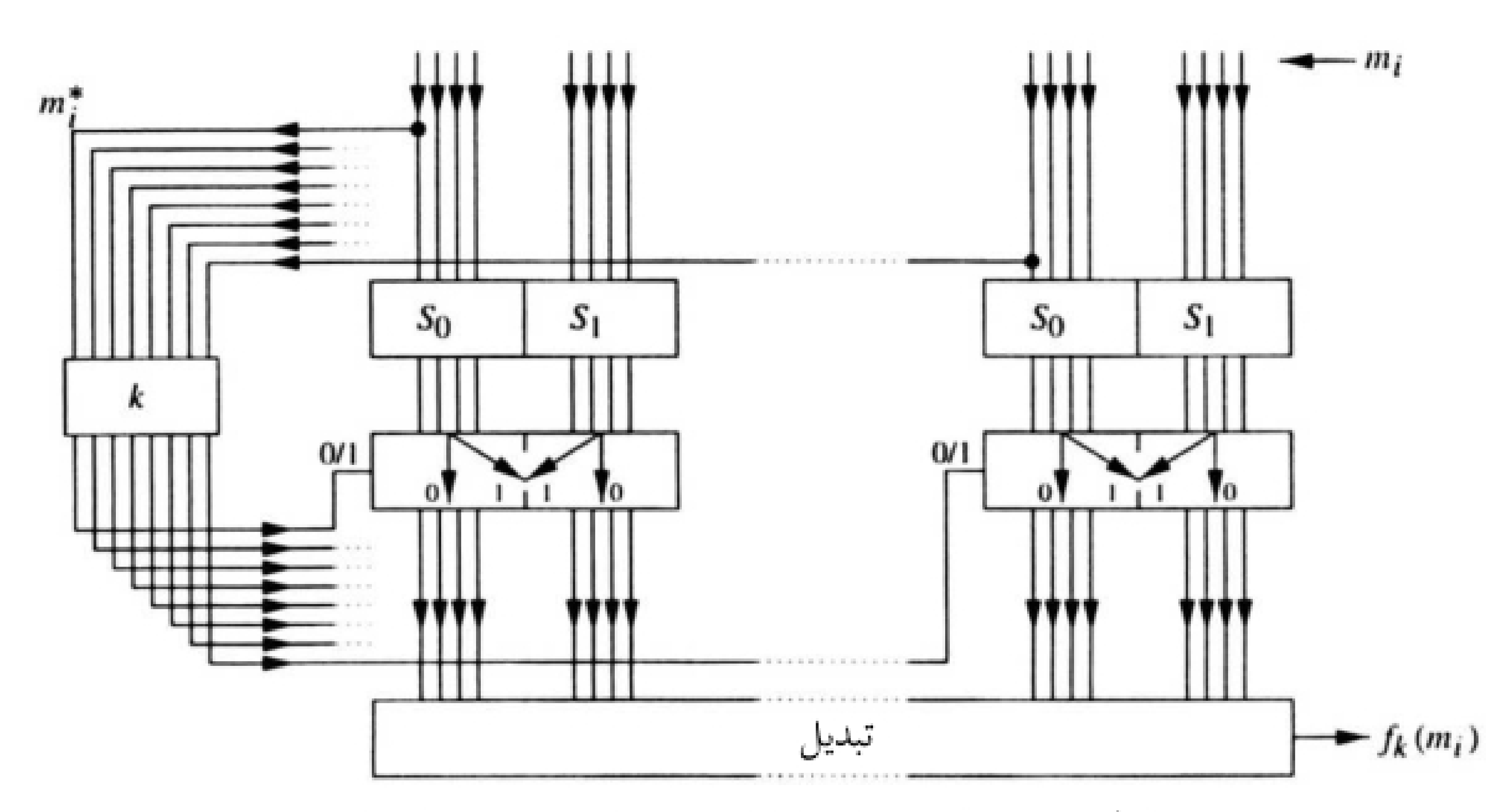
(١) نقوم بتجزئة m_i إلى 8 بايتات طول كل منها 8 مراتب ونفرض أن m_i^* هي البايت التي نحصل عليها من المرتبة الأولى لكل من بايتات m_i .

(٢) نقوم بتجزئة كل من بايتات m_i إلى كلمتين طول كل منها يساوي 4 ثم نجعل الدالة S_0 تؤثر على النصف الأيسر و S_1 تؤثر على النصف الأيمن.

(٣) إذا كانت المرتبة j من $k\left(m_i^*\right)$ تساوي 1 فنقوم بتبديل نصفي البايت j لمخرج $S_0 S_1$.

(٤) نستخدم تبديلاً ثابتاً (غير سري) لتبديل المراتب المخرجة والتي عددها 64 .

يبين الشكل (١٠,٣) مرحلة من مراحل NDS حيث التبديل النهائي يمنع من تقسيم الخطة إلى ثمان خطط أصغر مستقلة.



الشكل (١٠,٣). الدالة f في مرحلة من مراحل NDS .

كسر نظام NDS باختيار النص الواضح

إن أحد عيوب نظام NDS هو استخدام المفتاح نفسه في جميع المراحل مما يقود إلى معرفة المفتاح ثم كسر النظام باختيار النص الواضح، ويتم ذلك على النحو التالي :

نفرض أن $T = T_k$ هو التحويل المقابل لمرحلة من مراحل NDS. أي أن :

$$T\left(m_{i-1}, m_i\right) = T_k\left(m_{i-1}, m_i\right) = \left(m_i, m_{i-1} \oplus f_k\left(m_i\right)\right)$$

ولنفرض أن $F = T^{16}$ يرمز للمراحل الـ 16 جميعاً. الملاحظة الأهم هنا هو أن F يتبدل مع T وذلك لأن :

$$.FT\left(m\right) = T^{16}T\left(m\right) = TT^{16}\left(m\right) = TF\left(m\right)$$

وبافتراض أن محلل التعمية على علم بالنظام المستخدم (من مبدأ كيرتشوف) ومن ثم يتم كسر النظام إذا استطاع الحصول على المفتاح k .

وبفرض أن $q \in \left\{0,1\right\}^8$ فيكون بإمكان محلل التعمية معرفة المفتاح إذا استطاع معرفة $k\left(q\right)$ لكل $q \in \left\{0,1\right\}^8$. ولانجاز ذلك يقوم بتنفيذ الخطوات التالية :

(١) يقوم بطمر q في الرسالة $m = \left(m_0, m_1\right)$ بحيث يكون $m_1^* = q$. وبهذا يحصل على النص المعمى $\left(m_{16}, m_{17}\right) = F\left(m\right)$ المقابل للنص الواضح المختار m.

(٢) لنفرض أن $\tilde{k}$ هي إحدى بايتات $k\left(q\right)$ وعددها 2^8. ولنفرض أن $\widetilde{T} = T_{\tilde{k}}\left(m\right)$ هو صورة الرسالة عند مرحلة واحدة تحت تأثير $\tilde{k}$.

(٣) إذا كانت $\tilde{k} = k\left(q\right)$ فنرى أن $\widetilde{T} = T\left(m\right)$ وأن:

$$F\left(\widetilde{T}\right) = FT\left(m\right) = TF\left(m\right) = T\left(m_{16}, m_{17}\right) = \left(m_{17}, ?\right)$$

وبهذا نجد أن النصف الأيسر من $F\left(\widetilde{T}\right)$ يتفق مع النصف الأيمن من $F\left(m\right)$. ويكون بإمكان محلل التعمية (العدو) الحصول على النص المعمى $F\left(\widetilde{T}\right)$ المقابل للنص الواضح المختار $\widetilde{T}$. وعليه، إذا كان النصف الأيمن من $F\left(m\right)$ يساوي النصف الأيسر من $F\left(\widetilde{T}\right)$ فيمكن اعتبار أن $\widetilde{T}$ تساوي $T\left(m\right)$ ومن ثم يقبل $\tilde{k}$ على أنه قيمة $k\left(q\right)$. لاحظ أن محلل التعمية يحتاج لتجريب $2^8 = 256$ قيمة للمفتاح $\tilde{k}$ على الأكثر ليحصل على مثل هذا التطابق.

وبتطبيق هذه الخطوات على كل $q \in \left\{0,1\right\}^8$ نحصل على مفتاح مرشح k باختيار $2^8\left(2^8 + 1\right) = 65792$ نصاً واضحاً على الأكثر.

من الممكن أن نحصل على المفتاح الخطأ k حيث من المحتمل أن يكون $\widetilde{T}$ (في الخطوة ٣) "مطابقاً" دون أن تكون قيمته مساوية للمقدار $T\left(m\right)$. ومع ذلك إذا كان النظام مصمماً بحيث يضيف تشويش ونشر فمن الممكن افتراض عدم وجود أكثر من قيمة $\tilde{k}$ لنحصل على التطابق.

نحتاج أيضاً في الخطوة (٣) أن يكون $\tilde{k} = k\left(q\right)$ عندما يكون $\widetilde{T} = T\left(m\right)$. والمجهول الوحيد عند حساب $T\left(m\right)$ في هذه المرحلة هو شرط تبديل $k\left(m_1^*\right)$ على مخرج التحويليين S_0 ، S_1. فإذا اتفق مخرج S_0 و S_1 على إحدى بايتات m_1 فلا يمكن

تحديد مرتبة $k\left(m_1^*\right)$ المقابلة بمعرفة $T\left(m\right)$. وبناء على ذلك، نحتاج إلى اختيار m بحيث يختلف مخرج S_0 و S_1 عند كل بايت من بايتات m_1 إضافة إلى كون أن $m_1^* = q$ (عدم التمكن من اختيار مثل هذا الـ m يعدُّ مؤشراً على إمكانية كسر النظام بأسلوب أسهل)

مثال توضيحي

نأخذ نظام شبيه بنظام NDS حيث $n = 4$ وعدد المراحل هو $r = 3$. طول الرسائل هو $2n = 8$ مرتبة ودالة المفتاح هي $k : \left\{0,1\right\}^2 \to \left\{0,1\right\}^2$. (كل من المفاتيح الجزئية الثلاثة يساوي k). سعة فضاء المفاتيح هي $\left(2^2\right)^{2^2} = 256$. لنفرض أن S_0 هو التحويل المحايد وأن S_1 هو التحويل المتمم (على كل مرتبة). التبديل هو كتابة المراتب بالترتيب العكسي. والمخطط الشبيه في مخطط الشكل (١٠,٣) يحتوي على صندوقين S_0 و S_1 كل منهما يقبل مرتبة واحدة من مراتب m_i والتي عددها $n = 4$.

لنفرض أن المفتاح k معرف على النحو التالي:

$$k\left(00\right) = 10 \text{ ، } k\left(10\right) = 11 \text{ ، } k\left(01\right) = 00 \text{ ، } k\left(11\right) = 10$$

وأن الرسالة المراد تعميتها هي $m = \left(m_0, m_1\right) = \left(0111,1100\right)$.

يتم حساب $m_2 = m_0 \oplus f\left(m_1\right)$ على النحو التالي:

$$m_1 = 1100 \xrightarrow{S_0S_1} 1001 \xrightarrow{k} 0110 \xrightarrow{\text{تبديل}} 0110 \xrightarrow{\oplus m_0} 0001 = m_2.$$

والمراحل الأخرى مشابهة، وبهذا نحصل على:

$$\begin{aligned}\left(m_0, m_1\right) &\mapsto \left(0111,1100\right) \mapsto \left(1100,0001\right) \mapsto \left(0001,1101\right) \\ &\mapsto \left(1101,0011\right) = \left(m_3, m_4\right) = F\left(m\right)\end{aligned}$$

سنوضح كسر النظام باختيار النص الواضح والحصول على $k\left(q\right)$ للحالة $q = 10$.

(١) نريد اختيار $m = (m_0, m_1)$ حيث $m_1^* = q$ بحيث تختلف مخرجات S_0 و S_1 عند التأثير على نصفي الرسالة m. فإذا اخترنا $m = (0111,1100)$ فنجد أن $F(m) = (1101,\underline{0011})$.

(٢) الجدول التالي يوضح مرحلة تعمية لقيم $\widetilde{T}$، قيمة لكل تخمين $\tilde{k}$ للمفتاح $k(q)$. كما يوضح الجدول القيم $F(\widetilde{T})$ المقابلة لكل خيار $\widetilde{T}$ للنص الواضح.

$\tilde{k}$	00	01	10	11
m_1	1100	1100	1100	1100
S_0S_1	1001	1001	1001	1001
تأثير $\tilde{k}$	1001	1010	0101	0110
تبديل	1001	0101	1010	0110
$\oplus m_0$	1110	0010	1101	0001
$\tilde{T}$	(1100, 1110)	(1100, 0010)	(1100, 1101)	(1100, 0001)
$F(\tilde{T})$	(0000, 1011)	(1100, 0100)	($\underline{0011}$, 1000)	($\underline{0011}$, 1011)

(٣) سنعتبر أن $\widetilde{T}$ هو النص المطابق إذا تساوي نصف $F(\widetilde{T})$ الأيسر مع نصف $F(m) = (1101,0011)$ الأيمن. وبالنظر إلى الجدول نجد هذا يحدث لقيمتين هما $(0011,1000)$ و $(0011,1011)$. ومن ثم نحصل في هذه المرحلة على قيمتين محتملتين للمفتاح $k(q)$ هما $\tilde{k} = 10$ و $\tilde{k} = 11$.

يوضح لنا هذا المثال احتمال فشل هذا الهجوم في تحديد قيمة وحيدة للمفتاح. ومن الممكن تجريب نصوص واضحة أخرى. على سبيل المثال، إذا كانت $m = (0101,1100)$ فسنجد قيمة وحيدة $\tilde{k} = 11$ على أنها القيمة الصحيحة للمقدار $k(10)$. ▲

تمارين

(**١٠,٣,١**) إذا كانت $c = (m_{r+1}, m_r) = (1111,0100)$ هي مُخرج التعمية في المثال التوضيحي فجد الرسالة المقابلة m.

(**١٠,٣,٢**) استخدم خطوات المثال التوضيحي لإيجاد $k(00)$.

(١٠,٣,٣) لتكن $f_1, f_2 : \{0,1\}^4 \to \{0,1\}^4$ دالتين معرفتين على النحو التالي:

$$f_1(x_1, x_2, x_3, x_4) = (x_2 \oplus x_4, 1, x_1 x_2, 1 \oplus x_3)$$
$$f_2(x_1, x_2, x_3, x_4) = (1, x_1 \oplus x_3, x_4, x_2)$$

لنفرض أن F نظام فيستل توضيحي معرف على النحو التالي:

- $n = 4$ (ومن ثم فطول الرسالة هو $2n = 8$ مرتبة)، عدد المراحل هو $r = 2$.
- مفتاح F هو زوج (k_1, k_2) من المراتب الثنائية.
- نستخدم الدالة f_{k_i} في المرحلة $i \in \{1,2\}$.

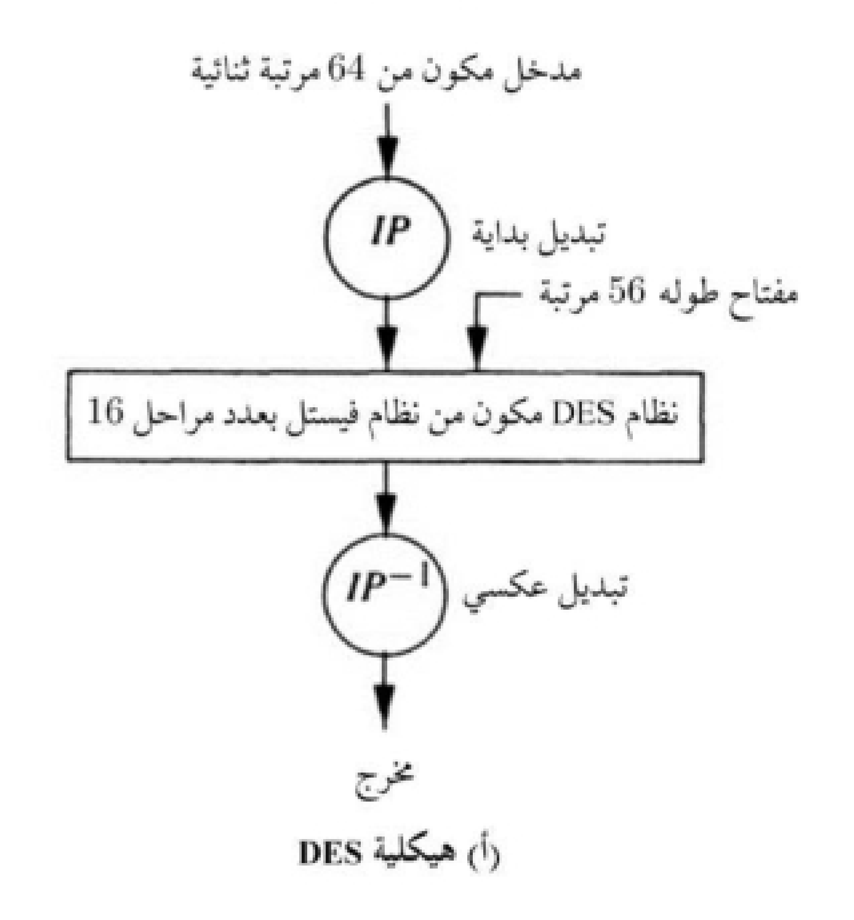
لنفرض أن c هو النص المعمى المقابل للنص الواضح m حيث مفتاح التعمية هو $(0,1)$. إذا كان:

$$c = m_{r+1} m_r = 10101011$$

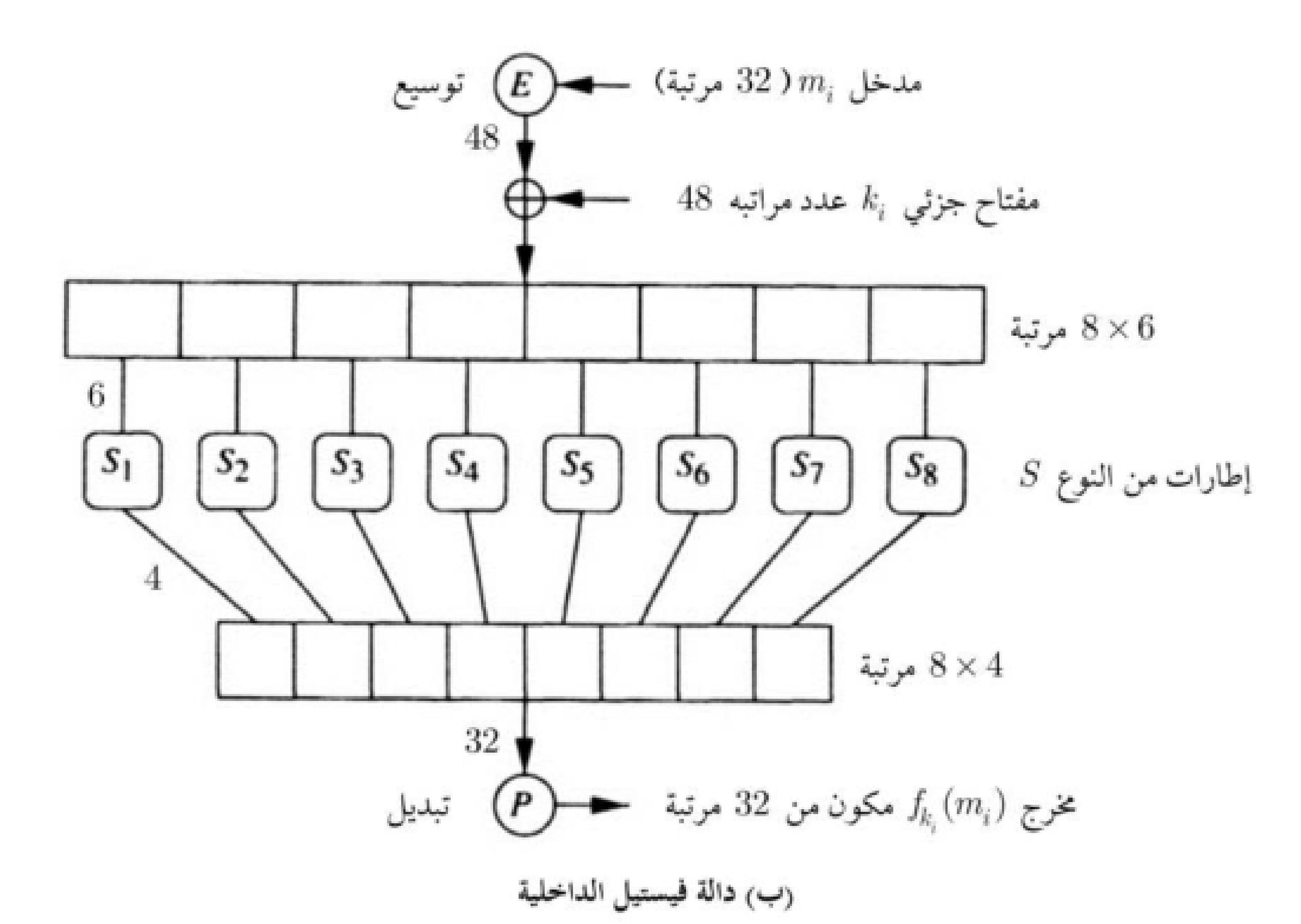
فجد النص الواضح m.

(١٠,٣,٢) نظام تعمية البيانات القياسي

بعد إعلان المعهد الوطني للقياس والتقنية National Institute of Standard) NIST and Technology) في العام ١٩٧٣م عن حاجته إلى نظام تعمية ليكون النظام الوطني القياسي قامت شركة IBM بالتعاون مع وكالة الأمن القومي (National Security Agency) بتطوير نظام يعتمد على نظام فيستل واعتمد النظام الجديد ليصبح نظام تعمية البيانات القياسي أو اختصاراً DES وكان ذلك في العام ١٩٧٧م. يستند نظام DES على نظام فيستل مكون من 16 مرحلة وطول المدخل يساوي 64 مرتبة ثنائية. يولّد جدول المفاتيح مفاتيح جزئية k_i طول كل منها 48 مرتبة ثنائية في كل مرحلة من مفتاح معطى k طوله 56 مرتبة ثنائية. يُثَبِّت النظام ثمانية دوال إطار من النوع S وهي دوال أساسية لأمن النظام ومبينة في الشكل (١٠,٤).



(أ) هيكلية DES



(ب) دالة فيستيل الداخلية

الشكل (٤,١٠). مخطط نظام تعمية البيانات القياسي.

أحدث ظهور نظام DES في العام ١٩٧٧م تطوراً مهماً في علم التعمية حيث أصبح من أوسع أنظمة التعمية ذات المفتاح المتماثل استخداماً. وحصل بعض اللغط حول الاصطلاح "القياسي" وأحد أسباب هذا اللغط هو بقاء بعض أجزاء التصميم

سرية مما قاد البعض إلى الاعتقاد بوجود دالة ذات باب سري (trapdoor function) تتيح لوكالة NSA من كشف الرسائل المعماة.

واجهت سعة فضاء المفاتيح العديد من العقبات خلال فترة استخدامه حيث إن خطة التعمية معلنة ومن ثم فأمن النظام يعتمد تماماً على المفتاح. طول المفتاح هو 64 مرتبة ثنائية منها ثمان مراتب مخصصة لاختبار النوعية مما يجعل الطول المؤثر للمفتاح 56 مرتبة ثنائية وحذر بعض الأكاديميين من احتمال كسر النظام من قبل محلل تعمية عنيد وبحوزته حاسبات آلية سريعة بطريقة استنفاد المفاتيح.

اقترح ديفي وهيلمان (Diffie and Hellman) في العام ١٩٧٧م تصميماً لآلة تستطيع كسر نظام DES بطريقة الاستنفاد بيوم كامل كلفتها 20 مليون دولار أمريكي (انظر [28]). وقدم مايكل واينر (Michael Wiener) في العام ١٩٩٣م تفاصيل تصميم آلة بإمكانها استنفاد فضاء المفاتيح بسبع ساعات وكلفتها مليون دولار أمريكي (انظر [93]) وتم تصميم نموذجاً آخر لهذه الآلة في العام ١٩٩٧م بإمكانها استنفاد فضاء المفاتيح بحوالي ساعة من الزمن (انظر [94]).

في شهر يناير من العام ١٩٩٧م أعلنت شركة RSA لأمن البيانات عن جائزة مقدارها عشرة آلاف دولار أمريكي لمن يتمكن من إيجاد مفتاح DES باستنفاد المفاتيح باختيار ثلاثة أزواج من النصوص الواضحة. وفي شهر يونيو من العام ١٩٩٧م (بعد خمسة أشهر) تمكنت مجموعة تدعى DES-CHALL من الحصول على الجائزة بالاستعانة بشبكة كبيرة من الحاسبات المرتبطة بالإنترنت. احتاج هذا الجهد الجماعي إلى 96 يوماً وسبعون ألف حاسب، واحتاج اكتشاف المفتاح إلى استنفاد حوالي 25% من فضاء المفاتيح. وفي العام ١٩٩٨م تم كسر النظام بأسلوب مماثل ولكن بزمن 40 يوماً واستنفاد 88% من فضاء المفاتيح. وقبل انتهاء هذا التحدي سجلت مجموعة رقم قياسي وهو استنفاد $34 \cdot 10^9$ مفتاحاً في كل ثانية بواسطة حوالي 1400 فريقاً.

استطاعت المؤسسة الرائدة للإلكترونيات (EFF) من الحصول على جائزة تحدي DES حيث استغرق إيجاد المفتاح إلى 56 ساعة من البحث باستخدام آلة مصممة لهذا الغرض بكلفة 200 ألف دولار وفي العام ١٩٩٩م تضافرت جهود مؤسسة EFF ومؤسسة الشبكة للتوزيع من كسر تحدي DES بزمن يساوي 22 ساعة واستنفاد 245×10^9 مفتاحاً في كل ثانية. راجت شائعات عن تعمد حكومة الولايات المتحدة الأمريكية من المبالغة في تكاليف هذه الآلة والاستخفاف من قدرة كسر النظام باختيار النص الواضح لغرض حماية مصالح أخرى. وكما علق ديفي بعد نشر التفاصيل الكاملة للبرامج الإلكترونية والتصميم لآلة كسر النظام الذي اكتشفها (انظر [34]) بقوله "إن السؤال لا يقتصر فقط على اكتشاف مفتاح DES بطريقة الاستنفاد؛ لأنه يجب الأخذ بعين الاعتبار كلفة ذلك والغرض من ذلك". إن إمكانية كسر نظام DES باستنفاد المفاتيح طريقة غير فعالة ويمكن الحصول على طريقة استنفاد فعالة إذا كان بحوزة محلل التعمية معلومات جزئية إضافية مثل البناء المستخدم أو بعض المعلومات عن النص الواضح.

من الممكن استخدام عمليات تعمية مضاعفة (سنناقش ذلك لاحقاً)؛ إضافة إلى DES وذلك لتحسين أمن النظام بطريقة الاستنفاد ولكن ذلك يكون على حساب سرعة التعمية (انظر التمرين (**١٠,٣,٥**)) ومع ذلك فنظام DES يعد من الأنظمة المحصنة حيث علق ديفي في رسالة إلى مؤسسة EFF (انظر [34]) بالقول "إن أي جدل مهما كان مقنعاً حول عدم أمن نظام DES لن يحد من الاستثمار الواسع في أدوات DES حول العالم وسيستمر العالم باستخدام نظام DES مهما كانت عيوبه لقناعتهم بملاءمته لاحتياجاتهم".

البديل المحتمل لنظام DES هو نظام التعمية القياسي المتقدم أو اختصاراً AES (Advanced Encryption Standard) حيث قدمت خوارزمية تعمية لهذا النظام في العام ٢٠٠٠م. يحاول هذا النظام تجنب نقاط ضعف نظام DES؛ وذلك بتحصنه عن محاولات

كسره باستنفاد المفاتيح. اقترح بعض علماء التعمية المشهورين (انظر [9]). إن استخدام مفتاح طوله 75 مرتبة ثنائية سيجعل النظام المستخدم آمناً للعام ١٩٩٦م وأن استخدام مفتاح طوله 90 مرتبة ثنائية سيضمن أمن النظام للعشرين سنة القادمة مع ملاحظة أن "تكلفة تعمية قوية لا تزيد كثيراً عن تكلفة تعمية ضعيفة".

التعمية المتكررة

من الممكن تنفيذ عملية التعمية عدداً من المرات في أنظمة التعمية القالبية مثل نظام DES بهدف الحصول على فضاء مفاتيح ذي سعة كبيرة. على سبيل المثال، تتم عملية التعمية المضاعفة على النحو التالي:

$E(M) = E_{k_2}E_{k_1}(m)$ حيث k_1 و k_2 مفتاحان.

ليس بالضرورة أن تعزز عملية التعمية المضاعفة من أمن النظام، وأحيانا لا تزيد حتى من طول المفتاح الفعال. إذا كان نظام التعمية مغلقاً تحت عملية التحصيل، أي إذا وجد $k_3 \in \mathcal{K}$ بحيث يكون $E_{k_2}E_{k_1} = E_{k_3}$ لكل $k_1, k_2 \in \mathcal{K}$ فلا يكون للتعمية المضاعفة أي تأثير على أمن النظام. على سبيل المثال، نظام التعويض البسيط حيث فضاء المفاتيح هو جميع التبديلات k على هجائية (انظر المثال (**١٠،٢،٢**)) مغلق تحت عملية التحصيل حيث $k_3 = k_2 \circ k_1$.

إذا كان k مفتاحاً لنظام DES فيكون DES_k تبديلاً على الهجائية $\{0,1\}^{64}$. ويحتوي فضاء المفاتيح على عدد من التبديلات لا يزيد عن 2^{56} (من مجموعة تبديلات عددها $2^{64}!$). وهذه المفاتيح (التبديلات) ليست مغلقة تحت عملية التحصيل ولهذا يستخدم النظام عمليات تعمية متعددة على أمل حمايته من الكسر بطريقة استنفاد المفاتيح.

في حالة عملية التعمية المضاعفة يكون على محلل التعمية (العدو) تجريب عدد من المفاتيح يساوي $2^{112} = \left(2^{56}\right)^2$. ومع ذلك فالنظام غير آمن بطريقة كسر تدعى طريقة الالتقاء بالمنتصف (meet-in-the-middle attack) حيث يكون على محلل التعمية

تجريب عدد من المفاتيح يساوي 2^{57} ولكن ذلك يأتي على حساب تخزين 2^{56} من المفاتيح.
إذا كان لدى محلل التعمية زوج واحد (m,c) على الأقل حيث $c = \mathrm{DES}_{k_2}\mathrm{DES}_{k_1}(m)$ فيستطيع معرفة المفتاحين k_1 و k_2 باتباع ما يلي:

(١) يقوم بعمل جدول للقيم $\left(i, \mathrm{DES}_i(m)\right)$ لجميع المفاتيح i.

(٢) لكل مفتاح محتمل j يبحث فيما إذا كان $\mathrm{DES}_j^{-1}(c)$ أحد عناصر القائمة. فإذا كان كذلك، فيوجد i حيث $\mathrm{DES}_j^{-1}(c) = \mathrm{DES}_i(m)$. وبهذا يكون $c = \mathrm{DES}_j \circ \mathrm{DES}_i(m)$. ومن ثم يجد أن $(i,j) = (k_1,k_2)$ هو أحد الخيارات المحتملة للقيمتين k_1 و k_2. وإذا توفر أزواج إضافية من النص الواضح وما يقابله من النص المعمى فبإمكان محلل التعمية استخدامها ليتخلص من التطابقات غير المنطقية. إذا كان بحوزة محلل التعمية زوجين من النصوص فيستطيع أن يكسر النظام.

يستخدم نظام DES عند التطبيق العملي له عمليات تعمية ثلاثية بفضاء مفاتيح سعته $2^{168} = \left(2^{56}\right)^3$ ودالة تعمية:

$$E(m) = E_{k_3}E_{k_2}E_{k_1}(m)$$

حيث $k_1,k_2,k_3 \in \mathcal{K}$ و $E_{k_i} = \mathrm{DES}_{k_i}$ أو $E_{k_i} = \mathrm{DES}_{k_i}^{-1}$.

كما يستخدم أحياناً حالة خاصة من عمليات التعمية الثلاثية (يستخدم مفتاحين) يكون فيها:

$$E_{k_2} = \mathrm{DES}_{k_2}^{-1} \quad \text{و} \quad k_3 = k_1 .$$

لاحظ أنه لو كان $k_2 = k_1$ لحصلنا على DES. إن عمليات التعمية الثلاثية تضمن أمن النظام ضد محاولة كسره بطريقة الالتقاء بالمنتصف حيث يحتاج لتجريب عدد 2^{112} من المفاتيح. ولكن من الممكن كسر الحالة الخاصة (استخدام مفتاحين) إذا استخدم محلل التعمية عدداً أكبر من النصوص الواضحة أو عمليات التعمية (انظر [63]).

أشكال العمليات

تقوم الأنظمة القالبية في الغالب بتقسيم النص الواضح إلى أجزاء (عادة تكون بنفس طول القالب) ثم يتم تعمية كل جزء على حدة. نستخدم نظام DES في الأمثلة التوضيحية مع التأكيد على أن هذه الطرق تصلح لجميع الأنظمة القالبية.

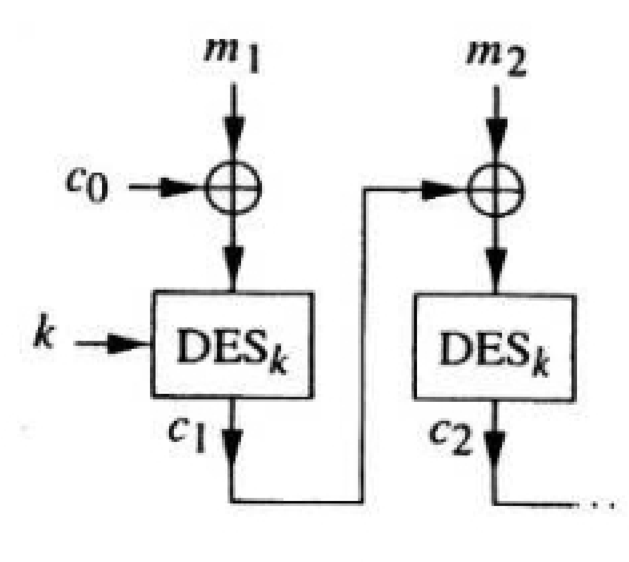
لنفرض أن $m = m_1 m_2 \ldots$ رسالة حيث m_i قالب (طوله 64 مرتبة في نظام DES). يقوم كتاب التعمية الإلكتروني (electronic codebook) أو اختصاراً ECB بتطبيق عملية DES على كل من هذه القوالب ليحصل على $c_i = \mathrm{DES}_k(m_i)$. ميزات هذه الطريقة هي سهولة تنفيذها وإذا حصل أخطاء في بعض مراتب قالب أثناء عملية التعمية فيبقى تأثير ذلك في القالب نفسه عند كشف المعمى. وأما العيب في هذه الطريقة هو أن النصوص الواضحة المتطابقة تعمى إلى نص معمى واحد وينتج عن ذلك تسريب بعض المعلومات لمحلل التعمية.

أما طريقة تعمية سلسلة قوالب (cipher-block chaining) أو اختصاراً CBC فتتم باختيار قالب بدائي c_0 وعملية التعمية تكون:

$$c_i = \mathrm{DES}_k(m_i \oplus c_{i-1}) \quad \text{لكل} \quad i \geq 1$$

وعملية كشف المعمى هي:

$$m_i = \mathrm{DES}_k^{-1}(c_i) \oplus c_{i-1}.$$



تعمية سلسلة قوالب

يتم اختيار القالب الأول من النص المعمى عشوائياً للحيلولة دون الحصول على النص المعمى نفسه للنصوص الواضحة المتطابقة. وتختلف هذه الطريقة عن ECB بوجود سلسلة جزئية من سلسلة تعتمد حدودها على الحدود السابقة حيث c_j يعتمد على c_{j-1} (وهذا بدوره يعتمد على جميع القوالب السابقة).

وكما رأينا فالأخطاء التي تحدث في النص المعمى c تؤثر فقط في قوالب كشف المعمى المقابلة للقوالب الذي حدثت في الأخطاء عند استخدامنا تعمية ECB، في حين CBC تقوم بنشر الخطأ في القالب c_j بحيث يمنع الحصول على كل من m_j و m_{j+1}. في الحقيقة، إذا حاول العدو التغيير في القالب c_j فإن ذلك يحدث أخطاء في مراتب m_{j+1} (انظر التمرين (**١٠,٣,٤**)).

تطبيقات على مطابقة الهوية

يمكن استخدام الأنظمة المتماثلة المفاتيح للحصول على تطابق الهوية (authentication). نقدم مثالين على هذه التطبيقات، أولهما، استخدام تعمية سلسلة القوالب (CBC) لتطابق هوية الرسالة وأما المثال الثاني فيستخدم خطة لكلمة سر (password) تعتمد على نظام DES لتطابق الهوية الشخصية (identification) وممكن أن يكون الفرق بين التطابقين غير واضح في معظم الأحيان، إلا أن تطابق هوية الرسالة تكون مهمته معرفة الرسالة الحقيقية وليس فقط معرفة الهوية.

مطابقة هوية الرسالة

لنفرض أن بوب (Bob) وأليس (Alice) يتبادلان رسائل عبر قناة اتصال غير آمنة (مثلاً، البريد الالكتروني). عند استلام بوب لرسالة مفترض أن تكون مرسلة من أليس يتوجب عليه أن يقتنع أن هذه الرسالة فعلا مرسلة من قبل أليس. يوجد على الأقل طريقتان لاعتراض الرسالة هما انتحال الشخصية أو التغيير في محتوى الرسالة (تزوير الرسالة).

إحدى الخيارات المتاحة للتحقق من هوية الرسالة هي استخدام خطة تعمية لنظام متماثل المفاتيح مثل DES ويتم ذلك على النحو التالي: يتفق كل من بوب وأليس على مفتاح سري مشترك، تقوم أليس باستخدام هذا المفتاح لتعمية الرسالة m وترسل $c = E_k(m)$ إلى بوب. يقوم بوب بكشف تعمية c باستخدام المفتاح المشترك ويقبل الرسالة إذا "اعتقد أن محتوى الرسالة معقول". ولمنع العدو من التلاعب في محتوى الرسالة بحيث يرسل إلى بوب رسائل بديلة، تقوم أليس بتذييل الرسالة m بمعلومات زائدة مثل الزمن أو أي متتالية من المعلومات الزائدة قبل تعميتها. فإذا كان من الصعب استخدام عملية التعمية بحيث يكون لكشف المعمى معنى مقبول دون معرفة المفتاح السري فنكون قد ضمنا مستوى ملائم لإعاقة العدو من تزييف محتوى الرسالة. ولكن بعض أنظمة التعمية تسمح ببعض التغييرات المختارة دون التمكن من كشف هذه التغييرات، على سبيل المثال، إذا استخدم ECB لتعمية قوالب من الرسائل فهناك احتمال أن يتمكن العدو من إعادة ترتيب أو تعويض أو حتى حذف بعض قوالب النص المعمى. أما نظام اللفافة الواحدة فيتيح للعدو تغيير بعض المراتب، وذلك بتغيير المراتب المقابلة لها في النص المعمى.

من الممكن استخدام خطط أقوى باستخدام نظام CBC ويتم ذلك باختيار نظام تعمية قالبي E وكتابة الرسالة $m = m_1m_2\dots m_t$ حيث طول m_i يساوي سعة النظام القالبي (إذا كان $E = \text{DES}$ فطول القوالب يساوي 64 مرتبة). نقوم الآن باستخدام CBC لحساب:

$$c_i = E_k(m_i \oplus c_{i-1}) \quad \text{لكل} \quad 1 \leq i \leq t.$$

بعد ذلك، ترسل أليس الرسالة m و c_t الذي يدعى شفرة مطابقة هوية الرسالة (message authentication code) أو اختصار BAC. يقوم الآن بوب بحساب CBC-MAC (بالطريقة نفسها التي حسبت بها أليس) ويقبل الرسالة على أنها المرسلة من أليس إذا

تساوت هذه القيمة مع قيمة MAC المستقبلة. ولمنع كسر النظام باستنفاد المفاتيح، يستخدم مفتاحاً آخر k' ويتم تعمية القالب الأخير باستخدام عملية تعمية ثلاثية باستخدام مفتاحين بحيث ترسل أليس $E_k E_{k'}^{-1}(c_t)$ عوضاً c_t وهذه تكون قيمة MAC.

مطابقة الهوية الشخصية

تعتمد خطة كلمة السر على معلومات سرية بين المستخدم ونظام الاتصال ولا يمكن الدخول إلى النظام إلا إذا قدم المستخدم السر المشترك للنظام. نقدم هنا آلية عمل كلمة السر المستخدمة في معظم أنظمة يونكس (Unix) للحاسبات. لكي تستطيع الدخول إلى النظام يتوجب عليك تقديم زوج من المعلومات هما هوية المستخدم وكلمة السر وبعد أن يتأكد النظام بواسطة معلومات مخزنة مسبقاً أن كلمة السر تقابل هوية المستخدم عندئذ، يسمح لك بالدخول إلى النظام.

تستخدم كلمة السر التي لا يزيد طولها عن 8 رموز في تكوين مفتاح k لدالة تعمية معدلة لنظام DES. كل من الرموز تساهم بعدد 7 من مراتب المفتاح التي عددها 56. يضاف مراتب صفرية إذا كان طول كلمة السر أصغر من 8 رموز. يضاف 12 مرتبة أخرى (تسمى الملح) تؤخذ من ساعة النظام في لحظة تكوين كلمة السر يكون الغرض منها تعديل نشر E في الشكل (**٤,١٠**) حيث يتم تحديد واحدة من التغييرات التي عددها $4096 = 2^{12}$. يقوم النظام بحساب $m_i = \mathrm{DES}_k^*(m_{i-1})$ لكل $1 \le i \le 25$ حيث DES^* يرمز لنظام DES المعدل و m_0 كلمة صفرية طولها 64 مرتبة. يتم تخزين كلمة الملح التي طولها 12 مرتبة والكلمة m_{25} التي طولها 64 مرتبة (تسمى كلمة السر المموهة) على النظام، عادة في الملف (/etc/passwd). وعند تقديم هوية المستخدم وكلمة السر يقوم النظام بإجراء الحسابات نفسها ويسمح للمستخدم في الدخول إلى النظام إذا كانت الحسابات متفقة مع القيمة المخزنة.

تدعى هذه الحسابات، خوارزمية تعمية كلمة السر باستخدام يونكس. يستطيع العدو الذي بحوزته مدخل من الملف (/etc/passwd) من محاولة كسر النظام بطريقة اختيار النص الواضح. وعلى الرغم من صعوبة كسر النظام باستنفاد المفاتيح فمن الممكن كسر النظام باستخدام قاموس لكلمات السر المعروف أنها مفضلة لدى المستخدمين. ولكن إضافة مراتب الملح تجعل كسر النظام باستخدام قاموس كلمات السر أكثر صعوبة لوجود 4096 خياراً لكل كلمة من كلمات السر. كما تساعد إضافة مراتب الملح على عدم السماح باستخدام تصميم غير قانوني لآلة نظام DES لكسر كلمة السر.

غالباً ما يكون باستطاعة العدو الحصول على الملف (/etc/passwd) نفسه (في عديدٍ من الأنظمة يستطيع جميع المستخدمين من قراءة هذا الملف)، ومن ثم يحاول كسر النظام بطرق مختلفة. إن معرفة بعض كلمات السر هو تهديد لا يستهان به حتى مع الأعداء الذين يستخدمون أجهزة ذات قدرة حسابية محدودة(٩). أجبر هذا الهجوم مستخدمي هذه الأنظمة إلى اختيار كلمات سر أفضل لمحاولة تحصين النظام من مثل هذا النوع من الهجوم وقاموا أيضاً بنقل كلمة السر المموهة إلى ملف منفصل تستلزم قراءته بعض المعلومات الإضافية.

تعدُّ خطة كلمة السر من الأمثلة على تطابق الهوية الضعيفة حيث لا يكون المستَخدِم على إطلاع مفصل عن هوية النظام المستخدَم، فإذا كانت القناة غير آمنة فمن الممكن انتحال العدو شخصية النظام إضافة إلى التصنت على عملية التعمية. نقدم في الفصل الثاني عشر المزيد عن تطابق الهوية.

---

(٩) استطاع كل من فيلدمير وكارن (Feldmeier and Karn) انظر [32] في العام ١٩٨٩م من استخدام قاموس كلمات السر لمعرفة 30% من كلمات سر نظام معطى حيث قدما خوارزمية كشف معمى سريعة في هذا الهجوم واستطاعا معرفة كلمات السر المموهة.

تمارين

(**١٠,٣,٤**) (أخطاء في النص المعمى لنظام DES) لنفرض أنه تمت تعمية t من قوالب النص الواضح $m_1, m_2, \ldots, m_t$ باستخدام نظام DES ونتج عن ذلك قوالب النصوص المعماة $c_1, c_2, \ldots c_t$ على التوالي.

(أ) لنفرض أنه تم إرسال نص معمى واحد يحتوي على أخطاء وليكن c_j. اشرح باختصار الطريقة التي يمكن إتباعها لتحديد عدد ومواقع القوالب التي يحتوي النص الواضح لها على أخطاء لكل من النظامين ECB و CBC.

(ب) لنفرض أن النظام المستخدم هو CBC ولنفرض أن العدو بدل موقعي القالبين c_3 و c_6. ماهو عدد قوالب النص الواضح التي تحتوي على أخطاء؟

(ج) بين كيف يمكن للعدو أن يُحدث أخطاء في بعض مراتب m_{j+1} بالتلاعب بالقالب c_j إذا كان النظام المستخدم هو CBC.

(**١٠,٣,٥**) تقترح هذه المسألة طريقة لحماية DES ضد محاولة كسره بطريقة استنفاد المفاتيح. المفتاح هو $k = (k_1, k_2)$ حيث $k_1 \in \{0,1\}^{56}$ و $k_2 \in \{0,1\}^{64}$. لنفرض أن $m \in \{0,1\}^{64}$ نص واضح.

(أ) أثبت أن استخدام الدالة $E_k(m) = \mathrm{DES}_{k_1}(m) \oplus k_2$ لا يزيد من أمن النظام عند محاولة كسره باستنفاد المفاتيح. أي بين كيفية كسر النظام باستخدام 2^{56} من عمليات DES. يمكن أن تفترض أن لديك عدداً معقولاً من الأزواج $(m_i, c_i = E_k(m_i))$.

(ب) هل يزيد استخدام دالة التعمية $E_k(m) = \mathrm{DES}_{k_1}(m \oplus k_2)$ من أمن النظام باستنفاد المفاتيح؟

اقترح رايسفت (Rivest) في مقالة المنشور في مجلة "CRYPTO, 96 [49]" التمديد DESX لنظام DES حيث $k = (k_1, k_2, k_3)$ ودالة التعمية هي:

$$E_k(m) = k_3 \oplus \mathrm{DES}_{k_1}(m \oplus k_2).$$

إضافة إلى أدوات DES المعروفة يسمح أيضا باستخدام العملية "XOR pre-and post" الرخيصة التكاليف.

(**١٠,٣,٦**) لنفرض أن حواء (العدو) حصلت على ثلاثة أزواج (m_1, c_1)، (m_2, c_2)، (m_3, c_3) حيث استخدمت أليس لتعميتهم نظام DES ثلاثي ودالة تعمية هي:

$$E(m) = \mathrm{DES}_{k_3}\mathrm{DES}_{k_2}\mathrm{DES}_{k_1}(m)$$

صمم هجوم اللقاء بالمنتصف لمعرفة مفتاح أليس (k_1, k_2, k_3) بعدد من العمليات يساوي تقريباً 2^{112}.

(**١٠,٣,٧**) (خاصية التتميم لنظام DES). لنفرض أن $\overline{m}$ هي متممة m (مرتبة مرتبة). إذا كان $c = \mathrm{DES}_k(m)$ فمن السهل أن نرى أن $\bar{c} = \mathrm{DES}_{\bar{k}}(\overline{m})$ (يمكن رؤية ذلك بالنظر إلى خطوات خوارزمية تعمية DES). هل من الممكن استخدام هذه الخاصية لتقليل الزمن اللازم لكسر النظام باستنفاد المفاتيح بطريقة معرفة النص الواضح؟ ماذا لو كانت الطريقة المستخدمة هي اختيار النص الواضح؟

(**١٠,٣,٨**) يقدم نظام CBC-MAC طريقة للتحقق من أمانة (صواب) المعلومات ولكنه لا يحافظ على سريتها. الاقتراح التالي يضيف المحافظة على السرية. نقوم بتذييل الرسالة $m = m_1 m_2 \dots m_t$ بـ MAC لنحصل على $m' = m m_{t+1}$. عندئذ يستخدم نظام CBC (باستخدام نفس المفتاح والقالب البدائي c_0) لتعمية m' لنحصل على النص المعمى $c_1, c_2, \dots, c_{t+1}$ حيث

$c_i = E_k(m_i \oplus c_{i-1})$ لكل $1 \leq i \leq t+1$ وحيث أول t من الحسابات مماثلة لتلك المستخدمة للحصول على MAC . وبهذا نحصل على النص المعمى مباشرة من الحسابات التي أجريت للحصول على MAC . أثبت أن هذه الخطة تؤدي إلى قالب نص معمى أخير $c_{t+1} = E_k(m_{t+1} \oplus c_t)$ لا يعتمد على النص الواضح ولا على النص المعمى. اشرح لماذا تؤدي هذه الإضافة في التعمية إلى خطر على أمن مطابقة الهوية ثم بين كيف يتمكن العدو من الاستفادة من هذا الضعف.

(٤,١٠) حواشي
Notes

الجملة الأولى في بداية هذا الفصل مأخوذة من كتاب رايسفت [71] الشيق "مقدمة في علم التعمية". يحتوي كتاب سايمنز (Simmons [81]) على إسهامات العديد من المؤلفين بما في ذلك إسهامات ديفي (Diffie [26]) "السنوات العشر الأولى للتعمية ذات المفتاح المعلن". ننصح بقراءة كتاب التعمية التطبيقية لمؤلفيه مينيزز، أورشت، فانستون (Menezes, van Oorshot, Vanstone [63]) لتغطيته المادة العلمية بشكل عميق ومنظم.

كتاب كاسر الشفرات لمؤلفه خان (Kahn) يحتوي على أدبيات التعمية غير التقنية لما قبل العام ١٩٦٧م، كما تضم الطبعة الثانية من الكتاب الذي صدر في العام ١٩٩٦م على بعض الإضافات عن تطور التعمية. يناقش غارفانكل (Garfinkel [37]) بعض الجوانب السياسية والقانونية والخصوصية ومسألة اتخاذ القرارات المتعلقة بالتعمية علاوة على تاريخ التطبيق "خصوصية جيدة وبارعة (Pretty Good Privacy (PGP))". أما كتابي ستنسون وكوبلتز (Stinson [86] and Koblitz [50]) فهما المكان الطبيعي لدراسة موسعة للمادة التي قدمناها في هذا الفصل.

يمكن الاطلاع على كمية هائلة من المعلومات عن المشروع (VENONA) الذي تبنته وكالة الأمن القومي على البوابة الإلكترونية:

http://www.nsa.gov

تبدأ المقدمة التاريخية بالفقرة التالية:

"بدأت في الأول من فبراير عام ١٩٤٣م خدمات مخابرات الإشارة التابعة للجيش الأمريكي وهو الاسم السابق لوكالة الأمن القومي برنامجاً سرياً صغيراً أطلقت عليه اسم حركي هو VENONA. كان الهدف الرئيسي لبرنامج VENONA هو متابعة وربما كسر أنظمة الاتصالات الدبلوماسية المعماة للاتحاد السوفيتي. بدأ تجميع هذه الرسائل من قبل خدمات مخابرات الإشارة (سميت لاحقاً وكالة الأمن القومي ويطلق عليها الاسم الشائع "ارلنغتون هول" نسبة إلى مكتبها الرئيسي في ولاية فرجينيا) منذ العام ١٩٣٩م ولكن لم يتم التحقق منها قبل ذلك. عينت المدرسة الشابة الآنسة جين غرابيل (Gene Grabeel) مسؤولة عن هذا المشروع."

الوصف المقدم لنظام البيانات الجديد المحكم (NDS) مأخوذاً من بيكر وبايبر (Berker and Piper [3]). ويمكن إيجاد تفاصيل نظام DES في المراجع [63, 86, 3]. من الممكن الرجوع إلى المقالات في سلسلة أعداد مجلة IEEE الذي بدأها [87] للاطلاع على الجدال حول أمن نظام DES. يمكن إيجاد بعض تصميمات الإطار S في المراجع [23]، [86] ، [76]. البوابة الإلكترونية:

http://www.rsa.com

تحتوي على معلومات عن التحدي الذي أطلقته مجموعة RSA لكسر النظام DES. أما محاولات كسر نظام DES فمن الممكن الاطلاع عليها على بوابة المؤسسة غير الربحية EFF:

http://www.eff.org

تم تبني استخدام DES CBS كنظام قياسي من قبل المنظمة العالمية للقياس (ISO 9797) والمعهد القومي الأمريكي للقياس (ANSI X9.9) لأغراض تطابق الهوية [63]

حيث أن استخدام ANSI X9.9 منتشراً بين البنوك وفي التعاملات المالية. تمت الموافقة على استخدام نظام DES الثلاثي من قبل ANSI في نوفمبر من العام ١٩٩٨م واعتمد نظاماً قياسياً (ANSI X9.52). وفي العام ١٩٩٩م بدأ المعهد القومي للقياس والتقنية (NIST) بإجراء التحضيرات لتبني نظام DES الثلاثي كنظام التعمية القياسي للمعلومات التابع للحكومة الفدرالية للولايات المتحدة الأمريكية (FIBS 46-3) انظر:

http://csrc.nist.gov/cryptval

ومن ضمن ما جاء بوثيقة الإعلان عن ذلك:

"بالإضافة إلى ذلك ولمعرفتنا أن ضمان أمن نظام DES يقترب من نهايته فقد تم التعاون بين NIST وقطاع الصناعة من جهة وبينهما وبين العاملين في قطاع علم التعمية لتطوير نظام تعمية قياسي متقدم (AES) يخدم القرن الواحد وعشرين. وقد بدأ هذا المشروع قيد التنفيذ في الثاني من يناير عام ١٩٩٧م (62 FR 93) حيث ينوي هذا المشروع إلى جعل خوارزمية التعمية لنظام AES غير سرية ومعلنة للعامة ولها القدرة على حماية ملفات الحكومة السرية إلى بداية القرن القادم. وبما أن خوارزمية تعمية أي نظام تحتاج لبعض الوقت للتأكد من قدرتها فلا بد من أخذ الوقت الكافي قبل طرح AES واعتباره نظام آمن من قبل FIBS. يمكن الحصول على معلومات عن الجهد المبذول من قبل NIST لتطوير AES على البوابة الإلكترونية":

http://www.nist.gov/aes

منذ فترة قصيرة تم تصميم آلة خاصة لكسر نظام DES وبناء على ذلك فقد تخلت NIST عن استخدام نظام DES للعديد من التطبيقات. وكما هو الحال مع أدوات الأمن الأخرى فالتعمية يجب أن توازن بين التكلفة وخطر كسر النظام. منذ فترة قصيرة تم بناء آلة كسر بكلفة 250000 دولار أمريكي واستطاعت معرفة مفتاح رسالة واحدة بحوالي 56 ساعة وذلك بإتباع طريقة الاستنفاد. ومن المتوقع أن يكون الزمن اللازم لكسر رسالة باستخدام مثل هذه التقنية الخاصة ضعف الزمن السابق؛ لأنه تم كسر النظام بالزمن السابق باستنفاد ربع المفاتيح فقط. في بعض التطبيقات لا يسبب مثل هذا

الكسر خطراً مباشراً، وخاصة عندما يحتاج المستخدم الحفاظ على سرية المعلومات لفترة زمنية قصيرة. ومن المتوقع مع التقدم في صناعة التقنية أن يتم كسر النظام بزمن أقل ولهذا توصي NIST بتبني المقترحات التالية:

- على الأنظمة المستخدمة تطوير استراتيجية انتقال حصيفة إلى نظام DES الثلاثي. يجب أن يكون لهذه الاستراتيجية القدرة على حماية المعلومات من الخطر المصاحب.
- عند بناء نظام جديد، استخدم نظام DES الثلاثي لحماية البيانات الحساسة ولكن غير السرية.

أخذت هذه الاقتراحات بعين الاعتبار عند الشروع في كتابة مسودة مشروع (FIPS 46-3) حيث تم اعتبار نظام DES الثلاثي كما هو مبين في (ANSI X9.52) على أنه الخوارزمية التي وافقت عليها FIPS.

الفصل الحادي عشر

موضوعات في الجبر ونظرية الأعداد
Topics in Algebra and Number Theory

يعتمد أمن أنظمة التعمية ذوات المفتاح المعلن على بعض مسائل نظرية الأعداد التي يعتقد أنها صعبة الحل. من هذه المسائل المشهورة مسألة تحليل الأعداد الصحيحة (FACTOR) ومسألة اللوغارتيم المنفصل (DLP):

FACTOR: جد تحليل العدد الصحيح الموجب n إلى عوامله الأولية.

DLP: ليكن p عدداً أولياً وليكن $\alpha \in \mathbb{Z}_p^*$ مولداً. إذا علمت $\alpha^x \pmod p$ فجد x.

وبتفصيل أكثر، تتطلب أي خطة تعمية للأنظمة ذوات المفتاح المعلن إلى مسألتين مترابطتين، إحداهما سهلة الحساب (التنفيذ) وأما الثانية فصعبة الحساب. على سبيل المثال، في مسألة تحليل الأعداد الصحيحة يكون من السهل نسبياً إيجاد حاصل الضرب $n = pq$ حيث p و q عددان أوليان ولكن المسألة العكسية وهي تحليل العدد n لإيجاد العددين الأوليين p و q فهي من المسائل غير المحلولة ويعتقد أنها صعبة حسابياً بصورة عامة.

نقدم في البنود التالية أربعة موضوعات هي الرواسب التربيعية، واختبار الأوليات، وتحليل الأعداد الصحيحة، واللوغاريتمات المنفصلة. هدفنا هو تقديم مادة

كافية من الجبر ونظرية الأعداد (وأيضاً خوارزميات نظرية الأعداد) لتكون أساساً لخطط تعمية أنظمة ذوات مفتاح معلن ، ولذا لن يكون شرحنا لهذه المادة مفصلاً.

(١١,١) الخوارزميات، تعقد الحسابات، حساب التطابقات
Algorithms, Complexity, and Modular Arithmetic

نقدم في هذا البند عدداً من الخوارزميات لتنفيذ العمليات الحسابية على الأعداد الصحيحة حيث تقاس فعالية هذه الخوارزميات بدلالة عدد العمليات الثنائية اللازمة لتنفيذ الخوارزمية. على سبيل المثال، إذا كان x و y عددين، عدد المراتب الثنائية لكل منهما يساوي k فنحتاج لتنفيذ $x+y$ إلى عدد من المراتب الثنائية لا يزيد عن k ونحتاج عدد من المراتب لا يزيد عن k^2 لتنفيذ xy (يوجد على الأكثر $k-1$ عملية جمع كل منها تحتاج إلى عدد k من العمليات الثنائية على الأكثر). وهذا العدد من العمليات الثنائية هو الأسوأ الذي نحصل عليه لجميع الأعداد الصحيحة التي عدد مراتبها الثنائية لا يزيد عن k. نستخدم عدد العمليات الثنائية ليكون المقياس للزمن اللازم لتنفيذ الخوارزمية على مدخل طوله k. يعتمد في العادة حساب الزمن اللازم على سعة المدخل وغالباً ما يعبر عن ذلك باستخدام رمز O الكبير (big-oh). لتكن f و g متتاليتين معرفتين على الأعداد الصحيحة الموجبة. نقول إن $f=O(g)$ إذا وجد عددان c و n_0. بحيث يكون:

$$\left|f(n)\right| \leq c\left|g(n)\right| \text{ لكل } n \geq n_0 .$$

على سبيل المثال، $f(n)=3n^4+7n-1=O(n^4)$ ، $\log n = O(n^t)$ لكل $t>0$. العبارة $f=O(1)$ تعني أن $\left|f\right|$ محدودة من الأعلى بثابت. في حالتي جمع وضرب عددين طول كل منهما k مرتبة ثنائية، يكون التعقد الحسابي هو $O(k)$ و $O(k^2)$

على التوالي. لاحظ أن العبارة $f(n)=O(2^n)$ لا تستبعد أن يكون $f(n)=O(n^2)$ وهي دالة تزايدها أبطأ بكثير من الدالة السابقة.

نقول إن خوارزمية لحساب عددين x و y طول كل منهما k هي خوارزمية حدودية (Polynomial time algorithm) إذا كان تعقدها الحسابي هو $O(k^t)$ حيث $t \in \mathbb{Z}$. سنعتبر الخوارزمية الحدودية على أنها خوارزمية فعالة (efficient) ولكن من المهم التنبيه أنه في بعض الأحيان تكون خوارزمية حدودية أبطأ من خوارزمية أسية لجميع قيم المدخلات المهمة.

لنفرض أن x و y عددان صحيحان حيث $0 \le x\,, y \le n$. عندئذ، يكون طول مدخل الخوارزمية هو عدد العمليات الثنائية $k=\lfloor \log_2 n \rfloor + 1$ في التمثيل الثنائي للعدد n. على وجه الخصوص، تكون الخوارزمية فعالة إذا كان زمن تنفيذها $O(k^t)$ وليس $O(n^t)$.

الأعداد الصحيحة

لنفرض أن $a,b \in \mathbb{Z}=\{0,\pm1,\pm2,\ldots\}$. نقول إن a يقسم b (a divides b) ونكتب $a \mid b$ إذا وجد عدد صحيح $c \in \mathbb{Z}$ حيث $b=ac$. على سبيل المثال، $-3 \mid 15$ لأن $15=(-3)(-5)$، كما أن أي عدد صحيح يقسم العدد 0. إذا وجد قاسماً $a \notin \{\pm1,\pm b\}$ للعدد b فنقول إن القاسم a غير تافه. نقول إن العدد الصحيح $a \ge 2$ عدد أولي (prime) إذا كانت جميع قواسمه تافهة، ويسمى العدد غير الأولي عدداً مؤلفاً (composite)، تقدم مبرهنة الأعداد الأولية (prime number theorem) تقريباً لعدد الأعداد الأولية $\pi(x)$ في الفترة $[2,x]$ وهذا التقريب هو $\pi(x) \sim x \,/\, \log x$. في الحقيقة هذا التقريب هو حد أدنى، على سبيل المثال، إذا كان $x=10^3$ فيكون:

$$\pi(x)=168 > x \,/\, \log x \approx 144\cdot 8\,.$$

من السهل التحقق من صحة الخواص التالية (تمرين (١١,١,٩)):

١- إذا كان $a \mid b$ و $b \mid c$ فإن $a \mid c$.

٢- إذا كان $c \mid a$ و $c \mid b$ (أي c قاسم مشترك للعددين a و b) فإن $c \mid (ax + by)$ لكل $x, y \in \mathbb{Z}$.

٣- إذا كان $p \mid ab$ حيث p عدد أولي فإن $p \mid a$ أو $p \mid b$.

نقول إن العدد $d \geq 0$ هو القاسم المشترك الأكبر (greatest common divisor) للعددين a و b ويكتب $d = \gcd(a, b)$ أو $d = (a, b)$ إذا كان $c \mid d$ لجميع القواسم المشتركة c للعددين a و b. تضمن لنا خوارزمية إقليدس (Euclidean algorithm) التي نقدمها لاحقاً وجود القاسم المشترك الأكبر دائماً. من الممكن استخدام المبرهنة الأساسية في الحساب (يمكن كتابة أي عدد صحيح $a \geq 2$ بطريقة وحيدة باستثناء الترتيب كحاصل ضرب أعداداً أولية) لإيجاد القاسم المشترك الأكبر. فمثلاً، إذا كان $36 = 2^2 \cdot 3^2$ و $24 = 2^3 \cdot 3$ فنرى أن $(36, 24) = 2^2 \cdot 3$.

إن مسألة تحليل العدد إلى حاصل ضرب عوامله الأولية تعدُّ من المسائل الصعبة ومع ذلك فمن الممكن إيجاد القاسم المشترك الأكبر دون الحاجة إلى التحليل. ولرؤية ذلك دعنا نقدم أولاً خوارزمية القسمة (division algorithm):

إذا كان $a, b \in \mathbb{Z}$ حيث $b \geq 1$ فمن الممكن استخدام القسمة المطولة لكتابة:

$$a = qb + r \quad \text{حيث} \quad 0 \leq r < b$$

العددان الصحيحان q (خارج القسمة) و r (الباقي ويكتب أحياناً $r = a (\operatorname{mod} b)$) هما عددان وحيدان. تستخدم خوارزمية إقليدس الحقيقة $(a, b) = (b, a (\operatorname{mod} b))$ حيث $a > b > 0$ لإيجاد القاسم المشترك الأكبر.

خوارزمية (١١,١,١) خوارزمية إقليدس

المدخل: عددان صحيحان $a \geq b \geq 0$.

المخرج: القاسم المشترك الأكبر (a, b) للعددين a و b.

(١) ضع $r_0 = a$ و $r_1 = b$.

(٢) جد أول عدد صحيح $n \geq 0$ يحقق $r_{n+1} = 0$ حيث $r_{i+1} = r_{i-1} \pmod{r_i}$.

أي أن r_{i+1} هو الذي نحصل عليه من خوارزمية القسمة $r_{i-1} = q_{i+1}r_i + r_{i+1}$.

(٣) $r_n = (a,b)$.

من الواضح أن خوارزمية إقليدس تتوقف دائماً لأن $0 \leq r_{i+1} < r_i$ لكل $i > 0$. في الحقيقة، $r_{i+2} < r_i / 2$ ومن ثم لا يمكن أن يزيد عدد عمليات القسمة عن $1 + 2\log_2 a$. عدد العمليات الثنائية لكل عملية قسمة هو $O(\log_2^2 a)$ ومن ثم يكون الزمن اللازم لتنفيذ خوارزمية إقليدس هو $O(\log_2^3 a)$ عملية ثنائية. ومن الممكن إثبات أن الزمن اللازم هو في الحقيقة $O(\log_2^2 a)$. وآيا كان الزمن المستخدم فخوارزمية إقليدس هي خوارزمية فعالة. التمرين (**١١,١,١١**) يثبت أن r_n هو بالفعل (a,b).

مثال (١١,١,٢)

في هذا المثال نستخدم خوارزمية إقليدس لحساب $(299,221)$ فنحصل على:

$$\begin{aligned}
(q_2 = 1, r_2 = 78) &\quad 299 = 1 \cdot 221 + 78 \\
(q_3 = 2, r_3 = 65) &\quad 221 = 2 \cdot 78 + 65 \\
(q_4 = 1, r_4 = 13) &\quad 78 = 1 \cdot 65 + 13 \\
(q_5 = 5, r_5 = 0) &\quad 65 = 5 \cdot 13 + 0
\end{aligned}$$

وبهذا يكون $13 = r_4 = (299,221)$. ▲

من الممكن استخدام خوارزمية إقليدس لكتابة (a,b) كتركيب خطي للعددين a و b. أي إيجاد عددين $x,y \in \mathbb{Z}$ بحيث يكون $(a,b) = ax + by$. يتم ذلك بخطوات ارجاعية لخوارزمية إقليدس (انظر الملحق A للاطلاع على التفاصيل). أول خطوتان هما:

$$\begin{aligned}
(a,b) = r_n &= r_{n-2} - q_n r_{n-1} \\
&= r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2}) \\
&= (1 + q_n q_{n-1})r_{n-2} - q_n r_{n-3}
\end{aligned}$$

ونحصل على (a,b) كتركيب خطي للعددين r_{n-2} و r_{n-3}.

تسمى هذه الطريقة خوارزمية إقليدس الموسعة حيث في الخطوة النهائية نحصل على (a,b) كتركيب خطي للعددين $r_0 = a$ و $r_1 = b$. وبتطبيق ذلك على المثال (١١,١,٢) نجد أن :

$$\begin{aligned}(299,221) = 13 &= 78 - 65 \\ &= 78 - (221 - 2 \cdot 78) = 3 \cdot 78 - 221 \\ &= 3(299 - 1 \cdot 221) - 211 = 3 \cdot 299 - 4 \cdot 221 \\ &= 3a - 4b\end{aligned}$$

حيث $a = 299$ و $b = 221$.

إذا كان $(a,b) = 1$ فنقول إن العددين a و b أوليان نسبياً (relatively prime). إذا كان $n \geq 1$ فعدد الأعداد الأولية نسبياً مع n في الفترة $[1,n]$ يرمز له بالرمز $\varphi(n)$ ويسمى دالة أويلر (Euler function). فمثلاً، $\varphi(6) = 2$ و $\varphi(p^i) = p^{i-1}(p-1)$ لكل عدد أولي p. دالة أويلر دالة ضربية. أي أن :

$\varphi(ab) = \varphi(a)\varphi(b)$ لكل a,b حيث $(a,b) = 1$.

على وجه الخصوص، $\varphi(pq) = (p-1)(q-1)$ لكل عددين أوليين p و q حيث $p \neq q$.

الأعداد الصحيحة قياس n

ليكن n عدد صحيح موجب. نقول إن a يطابق b قياس n ونكتب $a \equiv b(\bmod n)$ إذا كان $n \mid (a-b)$. فمثلاً، $14 \equiv 9(\bmod 5)$ ، $-11 \equiv 3(\bmod 7)$ ، $-1 \equiv n-1(\bmod n)$. التطابق هو علاقة تكافؤ على مجموعة الأعداد الصحيحة $\mathbb{Z}$. أي أن العلاقة :

- انعكاسية : $a \equiv a(\bmod n)$ لكل $a \in \mathbb{Z}$.
- تناظرية : إذا كان $a \equiv b(\bmod n)$ فإن $b \equiv a(\bmod n)$.
- متعدية : إذا كان $a \equiv b(\bmod n)$ و $b \equiv c(\bmod n)$ فإن $a \equiv c(\bmod n)$.

إذا كان $a = qn + r$ حيث $0 \leq r < n$ فنرى أن $a \equiv r(\operatorname{mod} n)$. من ذلك نجد أن كل $a \in \mathbb{Z}$ يطابق عدداً وحيداً في الفترة $[0, n-1]$. يحتوي فصل التكافؤ أو فصل التطابق أو نظام الرواسب التام $[a]$ على جميع الأعداد الصحيحة التي تطابق a قياس n. سنرمز لجميع فصول التطابق المختلفة قياس n بالرمز $\mathbb{Z}_n$.

من السهل أن نرى أن عمليتي الجمع والضرب على $\mathbb{Z}_n$ المعرفتين على النحو التالي:

$$[a] + [b] = [a + b]$$
$$[a][b] = [ab]$$

حسـنتا التعريـف، أي إذا كـان $a \equiv a'(\operatorname{mod} n)$ و $b \equiv b'(\operatorname{mod} n)$ فـإن $a + b \equiv a' + b'(\operatorname{mod} n)$ و $ab \equiv a'b'(\operatorname{mod} n)$. يكـون النظـام $(\mathbb{Z}_n, +, \cdot)$ حلقـة تحـت عملـيتي الجمـع والضـرب (تمـرين (**١١,١,١٢**)). في العـادة نكتـب $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ عوضًا عن $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ حيث قابلنا بين العنصر a وفصل التكافؤ $[a]$.

ليكن $a \in \mathbb{Z}_n$. إذا وجد $x \in \mathbb{Z}_n$ حيث $ax \equiv 1(\operatorname{mod} n)$ فنقول إن a قابل للعكس (invertible) وأن x هو معكوس (نظير ضربي) للعدد a ونكتب $x = a^{-1}$. فمثلاً $2^{-1} = 5$ في الحلقة $\mathbb{Z}_9$ لأن $2 \cdot 5 \equiv 1(\operatorname{mod} 9)$، أما الأعداد $\{0, 3, 6\}$ فليس لها معكوسات. إذا كان $a \in \mathbb{Z}_n$ قابلاً للعكس فنرى أن $ax \equiv 1(\operatorname{mod} n)$. أي أن $n \mid (ax - 1)$. ومن ذلك يكون $ax - ny = 1$ حيث $y \in \mathbb{Z}$. وبهذا يكون $(a, n) = 1$. وبالعكس، إذا كان $(a, n) = 1$ فيوجد $x, y \in \mathbb{Z}$ حيث $ax + ny = 1$. ومن ثم يكون $ax \equiv 1(\operatorname{mod} n)$. إذن، $a \in \mathbb{Z}_n$ قابل للعكس إذا وفقط إذا كان $(a, n) = 1$. وبهذه الحالة نستطيع استخدام خوارزمية إقليدس الموسعة لإيجاد معكوس a.

مثال (١١,١,٣)

لنفرض أن $a = 7$ و $n = 9$. العمود الأول من الجدول التالي يستخدم خوارزمية إقليدس ليبين أن $(7,9) = 1$ ومن ثم فللعدد a معكوس في الحلقة $\mathbb{Z}_9$. أما العمود الثاني فيجد $x, y \in \mathbb{Z}$ حيث $ax + ny = (a,n)$.

خوارزمية اقليدس الموسعة لكتابة $(a,n) = ax + ny$	خوارزمية اقليدس لإيجاد (a,n)
$1 = 7 - 3 \cdot 2$	$9 = 1 \cdot 7 + 2$
$= 7 - 3(9 - 1 \cdot 7)$	$7 = 3 \cdot 2 + 1$
$= 4 \cdot 7 - 3 \cdot 9$	$2 = 2 \cdot 1 + 0$

إذن، $7^{-1} = 4$ ومن السهل التحقق من أن $7 \cdot 4 \equiv 28 \equiv 1 (\bmod 9)$. ▲

مجموعة جميع أعداد $\mathbb{Z}_n$ القابلة للعكس $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : (a,n) = 1\}$ زمرة تحت عملية الضرب عدد عناصرها يساوي $\varphi(n)$. فمثلاً، $\mathbb{Z}_{12}^* = \{1,5,7,11\}$، $\mathbb{Z}_p^* = \{1,2,\ldots p-1\}$ حيث p أولي. إذا كان p عدداً أولياً وكان $a \in \mathbb{Z}_p^*$ فتنص مبرهنة فيرما الصغرى (Fermat's little theorem) على أن $a^{p-1} \equiv 1 (\bmod p)$ أما تعميم هذه المبرهنة فتسمى مبرهنة أويلر (Euler theorem) وهي $a^{\varphi(n)} \equiv 1 (\bmod n)$ لكل عدد صحيح $n \geq 2$ ولكل $a \in \mathbb{Z}_n^*$.

تعرف رتبة (order) العدد $a \in \mathbb{Z}^*$ وتكتب $ord(a)$ على أنه أصغر عدد صحيح موجب t يحقق $a^t \equiv 1 (\bmod n)$. يقدم التمرين (**١١,١,٢١**) بعض الخصائص الأساسية التي تتحقق في الزمرة $\mathbb{Z}_n^*$، إحدى هذه الخصائص هي أن $\mathrm{ord}(a) \mid \varphi(n)$ لكل $a \in \mathbb{Z}_n^*$.

إذا كانت رتبة $a \in \mathbb{Z}_n^*$ هي $\mathrm{ord}(a) = \left|\mathbb{Z}_n^*\right| = \varphi(n)$ فنقول إن a مولّداً (generator) للزمرة $\mathbb{Z}_n^*$. وفي هذه الحالة يكون $\mathbb{Z}_n^* = \{a^j : a \leq i < \varphi(n)\}$. من

المعلوم وجود مولدات للزمرة $\mathbb{Z}_p^*$ حيث p عدد أولي، فمثلاً من السهل التحقق من أن 2 مولّداً للزمرة $\mathbb{Z}_{13}^*$.

مثال (١١,١,٤)

اعتبر الزمرة $\mathbb{Z}_{15}^* = \{1,2,4,7,8,11,13,14\}$. عدد عناصر $\mathbb{Z}_{15}^*$ هو $\varphi(15) = \varphi(3)\varphi(5) = (3-1)(5-1) = 8$. رُتب هذه العناصر مبينة في الجدول التالي:

$a \in \mathbb{Z}_{15}^*$	1	2	4	7	8	11	13	14
$\operatorname{ord}(a)$	1	4	2	4	4	2	4	2

لاحظ أن $\operatorname{ord}(a)$ يقسم $\varphi(n) = 8$ لكل $a \in \mathbb{Z}_{15}^*$. لاحظ أيضاً عدم وجود مولّد للزمرة $\mathbb{Z}_{15}^*$؛ وذلك لعدم وجود عنصر من الرتبة 8. ▲

مبرهنة (١١,١,٥) مبرهنة الباقي الصينية

إذا كانت الأعداد الصحيحة $n_1, n_2, \ldots n_k$ أولية نسبياً مثنى مثنى فيكون لنظام التطابقات:

$$
\begin{aligned}
x &\equiv a_1 (\operatorname{mod} n_1)\\
x &\equiv a_2 (\operatorname{mod} n_2)\\
&\vdots\\
x &\equiv a_k (\operatorname{mod} n_k)
\end{aligned}
$$

حلاً وحيداً قياس $n = n_1 n_2 \ldots n_k$.

لنفرض أن $k = 2$ في مبرهنة الباقي الصينية. بما أن $(n_1, n_2) = 1$ فيوجد $s, t \in \mathbb{Z}$ حيث $sn_1 + tn_2 = 1$. التمرين (١١,١,١٨) يطلب التحقق من أن $x = (sn_1a_2 + tn_2a_1)(\operatorname{mod} n)$ هو الحل الوحيد للنظام. وكمثال على ذلك، نأخذ النظام:

$$
\begin{aligned}
x &\equiv 3 (\operatorname{mod} 7)\\
x &\equiv 6 (\operatorname{mod} 13)
\end{aligned}
$$

باستخدام خوارزمية إقليدس الموسعة نجد أن $(7,13) = 1 = 2 \cdot 7 - 1 \cdot 13$.
وبهذا فإن الحل الوحيد للنظام قياس $n = 7 \cdot 13 = 91$ هو $2 \cdot 7 \cdot 6 - 1 \cdot 13 \cdot 3 = 45$
. خوارزمية جاوس (Gauss) التالية تعمم لنا ذلك.

خوارزمية (١١,١,٦) جاوس

يمكن حساب الحل x لنظام تطابقات مبرهنة الباقي الصينية على النحو التالي:

$$x \equiv \sum_{i=1}^{k} a_i N_i M_i (\bmod n)$$

حيث $N_i = \frac{n}{n_i}$ و $M_i \equiv N_i^{-1} (\bmod n)$.

إن حساب $a^k (\bmod n)$ بطريقة فعالة مهم للعديد من خطط التعمية. من الممكن إنجاز ذلك بطريقة بدائية بحساب a^k ومن ثم قسمة الناتج على n أو بحساب $a^i (\bmod n)$ ، $i \le i \le k$ بعمليات ضرب متتالية. ولكن كل من هاتين الطريقتين غير فعالة سواء من ناحية سعة التخزين اللازمة أو عدد عمليات الضرب اللازمة. أما طريقة التربيع والضرب (Square-and-multiply) فهي طريقة فعالة لإجراء هذه الحسابات. ولاستخدام هذه الطريقة نقوم بإيجاد التمثيل الثنائي للعدد k وهو:

$$k = \sum_{i=0}^{t} k_i 2^i \quad \text{حيث} \quad t = \lfloor \log_2 k \rfloor$$

وبعد ذلك نجد:

$$a^k = \prod_{i=0}^{t} a^{k_i 2^i} = \left(a^{2^0}\right)^{k_0} \left(a^{2^1}\right)^{k_1} \ldots \left(a^{2^t}\right)^{k_t} = \prod_{k_i = 1} a^{2^i}.$$

لاحظ أن $a^{2^t} = \left(a^{2^{t-1}}\right)^2$. ولذا نحتاج لحساب $a^k (\bmod n)$ عدد t من التربيعات قياس n وعلى الأكثر t من عمليات الضرب قياس n. الخوارزمية التي نقدمها لحساب $a^k (\bmod n)$ يتم تنفيذها بعمليات ضرب جزئية. يمكن أيضاً الرجوع إلى [63] حيث توجد خوارزميات تربيع وضرب أخرى.

خوارزميات (١١,١,٧) خوارزمية التربيع والضرب

المدخلات: $0 \neq a \in \mathbb{Z}_n$ وعدد صحيح $0 \leq k < n$ والتمثيل الثنائي $k = \sum_{i=0}^{t} k_i 2^i$.

المخرج: $a^k \pmod n$.

(١) ضع $A \leftarrow a$ و $b \leftarrow 1$.

(٢) لكل i من 0 إلى t نفذ التالي:

(أ) إذا كان $i > 0$ فضع $A \leftarrow A^2 \pmod n$.

(ب) إذا كان $k_i = 1$ فضع $b \leftarrow bA \pmod n$.

(٣) توقف (b).

مثال (١١,١,٨)

نستخدم الخوارزمية لحساب $3^{26} \pmod{35}$. أي أن $a = 3$ وأن $n = 35$ وأن:

$$k = 26 = \sum_{i=0}^{4} k_i 2^i = 11010_2$$

الجدول التالي يبين حسابات الخوارزمية:

i	0	1	2	3	4
k_i	0	1	0	1	1
A	3	$3^2 \pmod n = 9$	$9^2 \pmod n = 11$	$11^2 \pmod n = 16$	$16^2 \pmod n = 11$
b	1	$1 \cdot 9 \pmod n = 9$	9	$9 \cdot 16 \pmod n = 4$	$4 \cdot 11 \pmod n = 9$

إذن $3^{26} \pmod{35} = 9$. في هذا المثال البسيط، يمكن التحقق وبسهولة من صواب الخوارزمية بحساب القوة قياس $\varphi(n) = \varphi(5 \cdot 7) = 24$ لنحصل على $3^k \pmod n = 3^2$. ▲

يلخص الجدول (١١,١) تعقد الحسابات للعمليات الأساسية في الزمرة $\mathbb{Z}_n$:

الجدول (١١,١). تحقق الحسابات في $\mathbb{Z}_n$ للعمليات الأساسية.

عدد العمليات الثنائية	العملية قياس n
$O(\log_2 n)$	الجمع : $a+b(\bmod n)$
$O\left((\log_2 n)^2\right)$	الضرب : $ab(\bmod n)$
$O\left((\log_2 n)^2\right)$	المعكوس : $a^{-1}(\bmod n)$
$O\left((\log_2 n)^3\right)$	القوة : $a^k(\bmod n)$ حيث $k<n$

تمارين

(١١,١,٩) أثبت خواص قابلية القسمة التالية :

(أ) $a \mid a$

(ب) إذا كان $a \mid b$ و $b \mid c$ فإن $a \mid c$.

(ج) إذا كان $a \mid b$ و $b \mid a$ فإن $a = \pm b$.

(د) إذا كان $c \mid a$ و $c \mid b$ فإن $c \mid (ax+by)$ لكل $x, y \in \mathbb{Z}$.

(١١,١,١٠) يُعرف المضاعف المشترك الأصغر (Least common multiple) ويكتب $\text{lcm}(a,b)$ للعددين الصحيحين الموجبين a و b على النحو التالي : $\text{lcm}(a,b) = \dfrac{ab}{(a,b)}$. إذا كان $a \mid c$ و $b \mid c$ فأثبت أن $\text{lcm}(a,b) \mid c$.

(١١,١,١١) هذا التمرين يتعلق بخوارزمية إقليدس (١١,١,١).

(أ) أثبت أن البواقي تحقق $r_{i+2} < r_i \,/\, 2$.

(ب) أثبت أن مخرج الخوارزمية هو بالفعل (a,b) .

(١١,١,١٢) يناقش هذا التمرين بعض الخواص الأساسية للحلقة $\mathbb{Z}_n$.

(أ) أثبت أن عمليتي الجمع والضرب على $\mathbb{Z}_n$ معرفتان تعريفاً حسناً.

(ب) أثبت أن $(\mathbb{Z}_n,+,\cdot)$ حلقة، استخدم خواص الحلقة $\mathbb{Z}$ لإثبات ذلك، على سبيل المثال تحقق من أن الضرب يتوزع على الجمع. أي أثبت أن :
$\big([a]+[b]\big)[c]=[a][c]+[b][c]$.

(**١١,١,١٣**) استخدم خوارزمية إقليدس لإيجاد $d=(105,180)$ ثم جد $x,y\in\mathbb{Z}$ بحيث يكون $105x+180y=d$.

(**١١,١,١٤**) استخدم خوارزمية التربيع والضرب لحساب $47^{332}(\operatorname{mod} 576)$.

(**١١,١,١٥**) أعط مثالاً مناقضاً لكل من العبارات الخاطئة التالية :

(أ) إذا كان $a,b,n\in\mathbb{Z}$ حيث $n\mid ab$ فإن $n\mid a$ أو $n\mid b$.

(ب) إذا كان $p\in\mathbb{Z}^+$ و $a\in\mathbb{Z}$ حيث $(a,p)=1$ فإن $a^{p-1}\equiv 1(\operatorname{mod} p)$.

(ج) إذا كان $a,b,c\in\mathbb{Z}$ فإن $(ab,c)=(a,c)(b,c)$.

(**١١,١,١٦**) جد رتبة كل عنصر من عناصر $\mathbb{Z}_{11}^*$ ثم حدد مولدات $\mathbb{Z}_{11}^*$.

(**١١,١,١٧**) لنفرض أن $a\in\mathbb{Z}_n^*$. أثبت أن جميع الأعداد $a^i(\operatorname{mod} n)$ حيث $0\le i<\operatorname{ord}(a)$ مختلفة.

(**١١,١,١٨**) أثبت الادعاء المذكور بعد مبرهنة الباقي الصينية (**١١,١,٥**) وهو أن $x\equiv(sn_1a_2+tn_2a_1)(\operatorname{mod} n)$ حيث $sn_1+tn_2=1$ حل للنظام المكون من التطابقين.

(**١١,١,١٩**) بين فيما إذا كان للنظام :

$$x\equiv 15(\operatorname{mod} 70)$$
$$x\equiv 104(\operatorname{mod} 151)$$

حلولاً أم لا. وبحالة وجود حلولاً للنظام فجد جميع هذه الحلول باستخدام خوارزمية إقليدس الموسعة.

(**١١,١,٢٠**) أثبت أن التطابق $ax\equiv b(\operatorname{mod} n)$ قابلاً للحل إذا وفقط إذا كان $(a,n)\mid b$. وإذا وجد حلول فعددها (a,n).

(١١,١,٢١) إذا كان $a \in \mathbb{Z}_n^*$ فأثبت صواب كل من العبارات التالية:

(أ) $a^x \equiv 1(\bmod n)$ إذا وفقط إذا كان $\mathrm{ord}(a) \mid x$. على وجه الخصوص $\mathrm{ord}(a) \mid \varphi(n)$.

(ب) $a^x \equiv a^y(\bmod n)$ إذا وفقط إذا كان $x \equiv y(\bmod \mathrm{ord}(a))$.

(ج) $a^x(\bmod n) = a^{x(\bmod \mathrm{ord}(a))}(\bmod n)$.

(١١,١,٢٢) ليكن p عدداً أولياً و $a \in \mathbb{Z}^+$. أثبت أن عدد حلول التطابق $x^a \equiv 1(\bmod p)$ في الحقل $\mathbb{Z}_p$ يساوي $(a, p-1)$.

(١١,١,٢٣) إذا كان p عدداً أولياً فأثبت أن جميع العناصر غير الصفرية في $\mathbb{Z}_p$ قابلة للعكس وأن $\mathbb{Z}_p$ حقلاً. تنص مبرهنة فيرما الصغرى على أن $a^{p-1} \equiv 1(\bmod p)$ حيث $a \in \mathbb{Z}_p^*$ ويمكن برهانها على النحو التالي:

(أ) افرض أن $T = \{a, 2a, \ldots, (p-1)a\} \subseteq \mathbb{Z}_p$. أثبت أن جميع عناصر T غير صفرية ومختلفة.

(ب) استخدم الفقرة (أ) لإثبات أن $T = \mathbb{Z}_p^*$. من ذلك يكون:

$$1 \cdot 2 \cdot \ldots \cdot (p-1) \equiv a(2a) \cdots (p-1)(a)(\bmod p)$$

الآن، أكمل البرهان باستخدام خوارزمية القسمة.

(١١,٢) الرواسب التربيعية
Quadratic Residues

افرض أن $a \in \mathbb{Z}_n^*$. نقول إن العدد a راسباً تربيعياً قياس العدد n (quadratic residue modulo) إذا وجد $x \in \mathbb{Z}_n^*$ حيث $x^2 \equiv a(\bmod n)$. وفي هذه الحالة نقول إن x هو جذر تربيعي للعدد a قياس n. إذا لم يكن a راسباً تربيعياً قياس n فنقول إنه ليس راسباً تربيعياً قياس n (quadratic nonresidue modulo n). سنرمز لمجموعة الرواسب التربيعية قياس n بالرمز Q_n ولمجموعة الرواسب غير التربيعية

قياس n بالرمز $\overline{Q_n}$. لاحظ أن $\mathbb{Z}_n^* = Q_n \cup \overline{Q_n}$. لاحظ إمكانية وجود عناصر $a \in \mathbb{Z}_n \setminus \mathbb{Z}_n^*$ بحيث يكون التطابق $x^2 \equiv a(\operatorname{mod} n)$ قابلاً للحل ولكن a ليس راسباً تربيعياً قياس n، على سبيل المثال، بأخذ $4 \in \mathbb{Z}_6$ وملاحظة أن $2^2 \equiv 4(\operatorname{mod} 6)$ نجد أن 2 حل للتطابق $x^2 \equiv 4(\operatorname{mod} 6)$ ولكن $2 \notin Q_6$ (لأن $4 \notin \mathbb{Z}_6^*$).

مبرهنة (١١,٢,١)

لنفرض أن $p > 2$ عدد أولي وأن α مولّد للزمرة $\mathbb{Z}_p^*$. عندئذ، يكون $a \in \mathbb{Z}_p^*$ راسباً تربيعياً قياس p إذا وفقط إذا وجد $i \in \mathbb{Z}$ بحيث يكون $a \equiv \alpha^{2i}(\operatorname{mod} p)$.

البرهان

إذا كان $a \equiv \alpha^{2i}(\operatorname{mod} p)$ حيث $i \in \mathbb{Z}$ فنرى أن $x = \alpha^i$ يحقق $x^2 \equiv a(\operatorname{mod} p)$ ومن ثم يكون a راسباً تربيعياً قياس p. ولبرهان العكس، نفرض أن $a \in Q_p$. عندئذ، يوجد $i \in \mathbb{Z}$ حيث $x \equiv \alpha^i(\operatorname{mod} p)$ حل للتطابق $x^2 \equiv a(\operatorname{mod} p)$ ومن ثم يكون $\alpha^{2i} \equiv a(\operatorname{mod} p)$. ■

نتيجة (١١,٢,٢)

لنفرض أن $p > 2$ عدد أولي وأن α مولّد للحقل $\mathbb{Z}_p^*$. عندئذ،

(١) $Q_p = \{\alpha^i(\operatorname{mod} p) : 0 \le i \le p-2$ و i زوجي$\}$ و $\overline{Q_p} = \{\alpha^i(\operatorname{mod} p) : 0 \le i \le p-2$ و i فردي$\}$.

(٢) $\left|Q_p\right| = \left|\overline{Q_p}\right| = \frac{p-1}{2}$.

(٣) إذا كان $a \in Q_p$ فيكون للتطابق $x^2 \equiv a(\operatorname{mod} p)$ حلان غير متطابقين فقط.

(٤) $\alpha^{\frac{p-1}{2}} \equiv -1(\operatorname{mod} p)$.

البرهان

نحصل على الفقرتين (١) و (٢) مباشرة من المبرهنة.

أما بالنسبة للفقرة الثالثة فلاحظ أولاً أن $\pm x$ حلان للتطابق وأن $x \not\equiv -x \pmod p$ (لأن $2x \not\equiv 0 \pmod p$ وأن p فردي و لا يقسم x)(*). ولبرهان الفقرة (٤)، لاحظ أولاً أن $\alpha^{\frac{p-1}{2}}$ حل للتطابق $x^2 \equiv 1 \pmod p$ لأن α من الرتبة $p-1$ وأن:

$$\left(\alpha^{\frac{p-1}{2}}\right)^2 = \alpha^{p-1} \equiv 1 \pmod p$$

وذلك استناداً إلى مبرهنة فيرما الصغرى. من ذلك نرى أن $\alpha^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$. وبما أن $ord(\alpha) = p-1$ فنرى أن $\alpha^{\frac{p-1}{2}} = -1 \pmod p$. ■

لنفرض أن $a \in \mathbb{Z}_p^*$. عندئذ، بتجريب عناصر المجموعة $\left\{x^2 \pmod p : x \in \mathbb{Z}_p^*\right\}$ يكون بمقدورنا معرفة فيما إذا كان $a \in Q_p$ أم لا. ولكن هذه الطريقة ليست فعالة حيث الزمن اللازم (في أسوأ الأحوال) لإنجاز ذلك يحتاج إلى $O(p)$ عملية ضرب. نستعين بالنتيجة السابقة للحصول على اختبار أكثر فعالية. يُعرف رمز ليجندر (Legendre symbol) ويرمز له بالرمز $\left(\frac{a}{p}\right)$ حيث $a \in \mathbb{Z}$ و $p > 2$ عدد أولي على النحو التالي:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & , p \mid a \\ 1 & , a \pmod p \in Q_p \\ -1 & , a \pmod p \notin Q_p \end{cases}$$

مبرهنة (١١,٢,٣) معيار أويلر

لنفرض أن $p > 2$ عدد أولي وأن $a \in \mathbb{Z}$. عندئذ،

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

(*) المترجمان: ولبرهان عدم وجود حلول أخرى غير متطابقة قياس p نفرض أن y_1 و y_2 حلان للتطابق. عندئذ، $p \mid (y_2^2 - y_1^2)$. أي أن $p \mid (y_2 - y_1)$ أو أن $p \mid (y_2 + y_1)$. إذن $y_2 \equiv y_1 \pmod p$ أو أن $y_2 \equiv -y_1 \pmod p$.

البرهان

سنبرهن الحالة $a \in Q_p$ ونترك الحالتين $a \in \overline{Q_p}$ و $a \mid p$ للتمرين (**١١,٢,١٠**).
لنفرض أن α مولّد للمجموعة $\mathbb{Z}_p^*$. عندئذ، يوجد $i \in \mathbb{Z}$ حيث $\alpha^{2i} \equiv a (\bmod p)$
وذلك استناداً إلى المبرهنة (**١١,٢,١**) وبهذا يكون:

$$a^{\frac{p-1}{2}} \equiv (\alpha^{2i})^{\frac{p-1}{2}} \equiv (\alpha^{p-1})^i \equiv 1 (\bmod p) \equiv \left(\frac{a}{p}\right) (\bmod p)$$

وذلك لأن $\left(\frac{a}{p}\right) = 1$. ■

إذا استخدمنا معيار أويلر لاختبار فيما إذا كان $a \in Q_p$ فنحتاج لحساب $a^{\frac{p-1}{2}}$ ويمكن إنجاز ذلك بعدد $O(\log_2^3 p)$ من العمليات الثنائية وذلك باستخدام خوارزمية التربيع والضرب، وهذه طريقة فعالة. لاحظ أن استخدام معيار أويلر يبين فقط فيما إذا كان $a \in Q_p$ أم لا ولكنه لا يجد الجذر التربيعي (على عكس عملية التجريب) للعدد a.

مثال (١١,٢,٤)

نستخدم معيار أويلر لاختبار فيما إذا كان $3 \in Q_p$ حيث $p = 23$. لحساب $3^{\frac{p-1}{2}} (\bmod p)$ لاحظ أن:

$$\frac{p-1}{2} = 11 = 1011_2 = \sum_{i=0}^{3} k_i 2^i$$

وباستخدام الخوارزمية (**١١,١,٧**) نجد أن الحسابات هي:

i	0	1	2	3
k_i	1	1	0	1
A	3	$3^2 = 9$	$9^2 (\bmod p) = 12$	$12^2 (\bmod p) = 6$
b	3	$3 \cdot 9 (\bmod p) = 4$	4	$4 \cdot 6 (\bmod p) = 1$

إذن، $\left(\frac{3}{p}\right) = 3^{\frac{p-1}{2}} (\bmod p) = 1$. وبهذا يكون $3 \in Q_{23}$ ويوجد x حيث $x^2 \equiv 3(\bmod 23)$.
سنقدم لاحقاً خوارزمية فعالة لإيجاد x. ولكن في هذا المثال السهل نرى وبسهولة أن $16^2 \equiv 3(\bmod 23)$. ▲

من الممكن أيضاً استخدام خصائص رمز ليجندر لحساب $\left(\frac{a}{p}\right)$ بطريقة أكثر فعالية من الطريقة المستخدمة في المثال (**١١,٢,٤**)، وسنوضح ذلك بعد تقديم تعميم لرمز ليجندر.

ليكن $n \geq 3$ عدداً صحيحاً فردياً حيث $n = p_1^{e_1} \dots p_k^{e_k}$ هو تحليل n إلى قوى عوامله الأولية ولنفرض أن $a \in \mathbb{Z}$. يرمز لرمز جاكوبي (Jacobi symbol) بالرمز $\left(\frac{a}{n}\right)$ ويعرف بدلالة رمز ليجندر على النحو التالي:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \dots \left(\frac{a}{p_k}\right)^{e_k}.$$

خواص رمز جاكوبي

نفرض أن $m, n \geq 3$ عددان صحيحان فرديان وأن $a, b \in \mathbb{Z}$. عندئذ:

(١) $\left(\frac{a}{n}\right) \in \{-1, 0, 1\}$ وأن $\left(\frac{a}{n}\right) = 0$ إذا وفقط إذا كان $(a, n) \neq 1$.

(٢) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$ و $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$.

(٣) إذا كان $a \equiv b(\bmod n)$ فإن $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(٤) $\left(\frac{1}{n}\right) = 1$ و $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1 & , n \equiv 1(\bmod 4) \\ -1 & , n \equiv 3(\bmod 4) \end{cases}$.

(٥) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1 & , n \equiv \pm 1(\bmod 8) \\ -1 & , n \equiv \pm 3(\bmod 8) \end{cases}$.

(٦) قانون المقلوب التربيعي (Low of quadratic reciprocity) :

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

باستخدام هذه الخواص لحساب $\left(\frac{3}{23}\right)$ المقدم في المثال (**١١,٢,٤**) نحصل على :

$$\left(\frac{3}{23}\right) = \left(\frac{23}{3}\right)(-1)^{\frac{3-1}{2}\cdot\frac{23-1}{2}} = \left(\frac{2}{3}\right)(-1)^{1\cdot 11} = -\left(\frac{2}{3}\right) = -(-1) = 1$$

وذلك لأن 23 أولي. وبهذا يكون $3 \in Q_{23}$ وهذا يتفق مع ما وجدناه باستخدام معيار أويلر.

إذا تمحصنا في تعريف رمز جاكوبي $\left(\frac{a}{n}\right)$ فنرى أننا نحتاج إلى تحليل n وهذه مسألة يعتقد أنها صعبة ومع ذلك فمن الممكن استخدام خواص رمز جاكوبي لحسابه دون اللجوء إلى التحليل.

مثال (١١,٢,٥)

باستخدام خواص رمز جاكوبي لحساب $\left(\frac{28}{55}\right)$ نحصل على :

$$\left(\frac{28}{55}\right) = \left(\frac{2}{55}\right)^2\left(\frac{7}{55}\right) \quad \text{(خاصية ٢)}$$

$$= \left(\frac{55}{7}\right)(-1)^{\frac{55-1}{2}\cdot\frac{7-1}{2}} \quad \text{(خاصية ٦)}$$

$$= -\left(\frac{55}{7}\right) = -\left(\frac{6}{7}\right) \quad \text{(خاصية ٣)}$$

$$= -\left(\frac{-1}{7}\right) - (-1)^{\frac{7-1}{2}} = 1 \quad \text{(خاصية ٤)}$$

ومع أن قيمة رمز جاكوبي يساوي 1 ، إلا أننا لا نستطيع الاستنتاج بأن 28 راسب تربيعي قياس 55 (في الحقيقة هو راسب غير تربيعي). وبملاحظة $28^{(55-1)/2} \equiv 52 \pmod{55}$

نرى أن معيار أويلر لا يتحقق للأعداد المؤلفة. وأخيراً، تذكر أن للراسب التربيعي قياس عدد أولي جذران. هنا $n = 55$ عدد مؤلف وأن الجذور التربيعية للعدد 1 قياس 55 هي ±1 و ±21 (سنناقش ذلك في البند (**١١,٤**)). ▲

كما رأينا في المثال السابق نجد أن $\left(\frac{a}{n}\right) = 1$ لا يحسم مسألة أن a راسب تربيعي أو راسب غير تربيعي قياس العدد المؤلف n. ومع ذلك إذا كان $a \in Q_n$ فيوجد $x \in \mathbb{Z}_n^*$ بحيث يكون $x^2 \equiv a(\bmod n)$ ومن ثم نجد أن $1 = \left(\frac{x}{n}\right)^2 = \left(\frac{x^2}{n}\right) = \left(\frac{a}{n}\right)$. وهذا يعني أنه إذا كان $\left(\frac{a}{n}\right) = -1$ فإن a راسب غير تربيعي قياس n. ولهذا السبب، إذا كان $n \geq 3$ عدداً صحيحاً فردياً نعرف المجموعة J_n على أنها:

$$J_n = \left\{a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) = 1\right\}$$

تسمى عناصر $\widetilde{Q_n} = J_n \setminus Q_n$ أشباه المربعات قياس n (pseudosquares module n).

لاحظ أن $Q_n \subseteq J_n$ وأن $Q_n = J_n$ عندما يكون n أولياً.

مثال (١١,٢,٦)

سنجد في هذا المثال الرواسب التربيعية وأشباه المربعات قياس العدد $n = 15$.

لاحظ أن $\left(\frac{a}{15}\right) = \left(\frac{a}{3}\right)\left(\frac{a}{5}\right)$ وأن:

$$\left(\frac{a}{3}\right) = \begin{cases} 1 & , a \equiv 1(\bmod 3) \\ -1 & , a \equiv 2(\bmod 3) \end{cases}$$

$$\left(\frac{a}{5}\right) = \begin{cases} 1 & , a \equiv \pm1(\bmod 5) \\ -1 & , a \equiv \pm2(\bmod 5) \end{cases}$$

الجدول التالي يبين قيم رمز جاكوبي $\left(\frac{a}{n}\right)$:

$a \in \mathbb{Z}_{15}^*$	1	2	4	7	8	11	13	14
$\left(\frac{a}{3}\right)$	1	−1	1	1	−1	−1	1	−1
$\left(\frac{a}{5}\right)$	1	−1	1	−1	−1	1	−1	1
$\left(\frac{a}{15}\right)$	1	1	1	−1	1	−1	−1	−1

إذن $J_{15} = \{1,2,4,8\}$. ومن السهل أن نجد أن $Q_{15} = \{1,14\}$. ولذا فإن أشباه المربعات هي $\widetilde{Q_{15}} = J_{15} \setminus Q_{15} = \{2,8\}$. ▲

ليكن $a \in J_n$. إن مسألة تحديد فيما إذا كان a راسباً تربيعياً أو شبه مربع قياس n ، تدعى مسألة الرواسب التربيعية (quadratic residuosity problem)، اختصاراً QRP. لنأخذ الحالة الخاصة $n = pq$ حيث p و q عددان أوليان مختلفان. سنطلب في التمارين إثبات أن $a \in J_{pq}$ راسب تربيعي إذا وفقط إذا كان $a \in Q_p$ و $a \in Q_q$ وأن:

$$\left|Q_{pq}\right| = \left|\widetilde{Q_{pq}}\right| = \frac{(p-1)(q-1)}{4}.$$

وبتطبيق ذلك على المثال (**١١,٢,٦**) نجد أن $\left(\frac{a}{5}\right) = 1 = \left(\frac{a}{3}\right)$ إذا وفقط إذا كان $a \in \{1,4\}$. وبهذا نجد أن $Q_{15} = \{1,4\}$ وأن $\left|Q_{15}\right| = 2 = \frac{(3-1)(5-1)}{4}$.

تمارين

(**١١,٢,٧**) جد كل من Q_{30} و $\widetilde{Q_{30}}$.

(**١١,٢,٨**) جد قيمة رمزي جاكوبي $\left(\frac{156}{235}\right)$ و $\left(\frac{1833}{587}\right)$. هل $156 \in Q_{235}$ ؟

(١١,٢,٩) جد الرواسب التربيعية وأشباه المربعات قياس العدد $n = 21$.

(١١,٢,١٠) أحد الزملاء غير الدقيقين ادعى أن " 36 راسب تربيعي قياس n لكل $n > 36$ لأن $36 = 6^2$ ". صحح هذا الادعاء وحدد فيما إذا كان $36 \in Q_{745}$.

(١١,٢,١١) لنفرض أن لدينا الخواص التالية لرمز ليجندر :

- $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ و $\left(\frac{-2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$ لكل عدد أولي فردي.
- إذا كان p و q عددين أوليين فرديين فإن :

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{(p-1)(q-1)}{4}}.$$

لنفرض أن $n \geq 3$ عدد صحيح فردي. أثبت خواص رمز جاكوبي التالية :

(أ) إذا كان n_1 و n_2 عددين صحيحين فرديين فأثبت أن :

$$\frac{n_1 n_2 - 1}{2} \equiv \frac{n_1 - 1}{2} + \frac{n_2 - 1}{2} \pmod 2.$$

استنتج أن $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$.

(ب) إذا كان n_1 و n_2 عددين صحيحين فرديين فأثبت أن :

$$\frac{n_1^2 n_2^2 - 1}{8} \equiv \frac{n_1^2 - 1}{8} + \frac{n_2^2 - 1}{8} \pmod 2.$$

استنتج أن $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$.

(ج) إذا كان $a \geq 3$ عدداً صحيحاً فردياً فأثبت أن :

$$\left(\frac{a}{n}\right) = \left(\frac{n}{a}\right)(-1)^{(a-1)(n-1)/4}.$$

(١١,٢,١٢) افرض أن p عدد أولي فردي. أثبت أن $-3 \in Q_p$ إذا وفقط إذا كان $p \equiv 1 \pmod 3$.

(١١,٢,١٣) أثبت استحالة أن يكون الراسب التربيعي مولّداً للمجموعة $\mathbb{Z}_p^*$.

(١١,٢,١٤) ليكن $n = pq$ حيث p و q عددان أوليان فرديان مختلفان.

(أ) أثبت أن $a \in Q_n$ إذا وفقط إذا كان $\left(\frac{a}{q}\right) = 1 = \left(\frac{a}{p}\right)$.

(ب) أثبت أن $\left|Q_n\right| = \frac{(p-1)(q-1)}{4}$. ارشاد: أثبت أن الدالة $f : Q_n \to Q_p \times Q_q$ المعرفة بالقاعدة $f(a) = (a \bmod p, a \bmod q)$ تقابل.

(١١,٢,١٥) أكمل برهان معيار أويلر (مبرهنة **(١١,٢,٣)**).

(١١,٣) اختبار الأوليات

Primality Testing

أحد المتطلبات الأساسية للعديد من أنظمة التعمية ذوات المفاتيح المعلنة هي توليد أعداد أولية كبيرة. ولذا فإحدى المسائل المطروحة هي اختبار فيما إذا كان العدد الصحيح $n > 2$ عدداً أولياً أم عدداً مؤلفاً. وبقسمة العدد على جميع الأعداد الأولية بين 2 و $\sqrt{n}$ يحدد فيما إذا كان العدد أولياً أم لا. كما أن هذه الطريقة تزودنا بعامل غير تافه إذا كان العدد مؤلفاً. ولكن هذه الطريقة ليست فعالة؛ لأنها تحتاج إلى $O(\sqrt{n})$ من عمليات القسمة.

في هذا البند نقدم اختباران احتماليان لأولية العدد هما اختبار سولوفي وستراسن (Solovay-Strassen test) واختبار ميلر ورابن (Miller-Rabin test). هذان الاختباران احتماليان؛ لأنه لو كان المخرج "مؤلف" يكون العدد n هو بالفعل مؤلف وإذا كان المخرج "أولي" فمن المحتمل أن يكون العدد مؤلفاً. ولهذا السبب فالتسمية الصحيحة لهذان الاختباران يجب أن تكون اختبارات أن يكون العدد مؤلفاً.

يعتمد اختبار سولوفي وستراسن على معيار أويلر (مبرهنة **(١١,٢,٣)**) والذي ينص على:

إذا كان n أولياً فإن $a^{(n-1)/2} \equiv \left(\dfrac{a}{n}\right) (\operatorname{mod} n)$. ويقترح علينا هذا المعيار التعريف التالي.

تعريف (١١,٣,١)

لنفرض أن n عدد صحيح فردي مؤلف وأن $1 \leq a < n$. إذا كان $(a,n) \neq 1$ أو كان $a^{(n-1)/2} \not\equiv \left(\dfrac{a}{n}\right) (\operatorname{mod} n)$ فنقول إن a شاهد أويلر على أن العدد n مؤلف (Euler witness to compositeness of n).

مبرهنة (١١,٣,٢)

ليكن n عدداً صحيحاً فردياً مؤلفاً وليكن $a \in \mathbb{Z}_n^*$ شاهد أويلر على أن العدد n مؤلف. عندئذ، على الأقل نصف عناصر $\mathbb{Z}_n^*$ هي شهود أويلر على n مؤلف.

البرهان

مجموعة غير الشهود $G = \left\{ x \in \mathbb{Z}_n^* : x^{(n-1)/2} \equiv \left(\dfrac{x}{n}\right) (\operatorname{mod} n) \right\}$ مغلقة تحت عملية الضرب في الزمرة المنتهية $\mathbb{Z}_n^*$. ولذا فهي زمرة جزئية من $\mathbb{Z}_n^*$. واستناداً إلى مبرهنة لاجرانج نرى أن $|G|$ يقسم $|\mathbb{Z}_n^*|$. وبما أن $a \in \mathbb{Z}_n^* \setminus G$ فنجد أن $|G| \leq |\mathbb{Z}_n^*| / 2$. ومن الممكن برهان المبرهنة بإثبات أن ab شاهد أويلر على أن العدد n مؤلف عندما يكون $b \in \mathbb{Z}_n^*$ ليس شاهدًا. وبهذا فعدد غير الشهود في $\mathbb{Z}_n^*$ هو على الأكثر $|\mathbb{Z}_n^*| / 2$. ■

مبرهنة (١١,٣,٣)

إذا كان n عدداً صحيحاً فردياً مؤلفاً فيوجد شاهد أويلر على أن العدد n مؤلف في $\mathbb{Z}_n^*$.

البرهان

لنفرض أولاً أن n ليس خالياً من المربعات. أي يوجد عدد أولي p حيث $p^2 \mid n$. ولنفرض أن $a = 1 + \dfrac{n}{p}$. عندئذ، $a \in \mathbb{Z}_n^*$ وأن:

$$\left(\frac{a}{n}\right)=\left(\frac{1+n\ /\ p}{(n\ /\ p)p}\right)$$

$$=\left(\frac{1+n\ /\ p}{n\ /\ p}\right)\left(\frac{1+n\ /\ p}{p}\right)$$

$$=\left(\frac{1}{n\ /\ p}\right)\left(\frac{1}{p}\right)=1$$

أيضاً، لدينا:

$$a^p \equiv \left(1+n\ /\ p\right)^p \equiv 1+\sum_{i=1}^{p}\binom{p}{i}\left(n\ /\ p\right)^i \equiv 1(\operatorname{mod} n)\ .$$

إذن، $ord(a)=p$ ؛ لأن $a\equiv 1(\operatorname{mod} n)$. وبما أن $p \not| (n-1)$ فنجد أن $a^{(n-1)/2} \not\equiv 1(\operatorname{mod} n)$. وبهذا يكون a شاهد أويلر على أن n مؤلف في هذه الحالة.

لنفرض الآن أن n حاصل ضرب أعداد أولية مختلفة. وليكن p قاسماً أولياً للعدد n و b راسب غير تربيعي قياس العدد p . باستخدام مبرهنة الباقي الصينية نستطيع إيجاد عدد a يحقق:

$$a \equiv b(\operatorname{mod} p)$$
$$a \equiv 1(\operatorname{mod} n\ /\ p)$$

وباستخدام خواص رمز جاكوبي نجد أن:

$$\left(\frac{a}{n}\right)=\left(\frac{a}{p(n\ /\ p)}\right)$$

$$=\left(\frac{a}{p}\right)\left(\frac{a}{n\ /\ p}\right)$$

$$=\left(\frac{b}{p}\right)\left(\frac{1}{n\ /\ p}\right)=-1$$

لأن b راسب غير تربيعي قياس p (لاحظ أن $a\in\mathbb{Z}_n^*$). الآن، من تعريف a نحصل على $a^{(n-1)/2}\equiv 1(\operatorname{mod} n\ /\ p)$ ومن ثم $a^{(n-1)/2}\not\equiv -1(\operatorname{mod} n\ /\ p)$.

إذن، $a^{(n-1)/2} \not\equiv -1 (\bmod n)$ ويكون a شاهد أويلر على أن n مؤلف في هذه الحالة أيضاً. ■

يمكن النظر إلى اختبار سولوفي وستراسن على أنه الاختبار الذي يبحث عن شاهد أويلر على n مؤلف وإذا لم يجد مثل هذا الشاهد فإنه يستنتج أن من المحتمل أن يكون n أولياً. ويستخدم عدد شواهد أويلر على أن n مؤلف للحصول على حد للخطأ.

خوارزمية (١١,٣,٤) اختبار سولوفي وستراسن

المدخل: عدد فردي $n > 2$ ووسيط $t \geq 1$.

المخرج: الإجابة "مؤلف" أو الإجابة "احتمال أولي".

(١) نفذ التالي على الأكثر t مرة:

(أ) اختار عدداً عشوائياً a حيث $1 < a < n$.

(ب) إذا كان $(a, n) \neq 1$ توقف "مؤلف".

(ج) إذا كان $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) (\bmod n)$ توقف "مؤلف".

(٢) توقف "احتمال أولي".

الزمن اللازم لتنفيذ العروة الداخلية يساوي $O(\log_2^3 n)$ عملية ثنائية. كتبنا خطوات الخوارزمية لأجل التوضيح مع ملاحظة أنه يمكن استبدال الخطوة (١,٢) بمقارنة $a^{(n-1)/2} (\bmod n)$ حيث نتوقف "مؤلف" إذا كانت القيمة لا تساوي 1 أو $n - 1$.

إذا كان مخرج الاختبار "مؤلف" فتمنح شهادة (certificate) تسمح من التحقق بطريقة فعالة على أن n هو بالفعل مؤلف. الشهادة في اختبار سولوفي وستراسن هي شاهد أويلر على أن n مؤلف وخوارزمية التحقق من ذلك هي التحقق من أن $(a, n) \neq 1$ أو أن $a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) (\bmod n)$. احتمال أن يكون مخرج الاختبار "احتمال أولي" عندما يكون n مؤلفاً لا يزيد عن 2^{-t}.

يمكن استخدام اختبار سولوفي وستراسن (أو اختبار ميلر ورابن المقدم في التمارين) لتوليد أعداد احتمال أن تكون أولية كبيرة جداً على النحو التالي: اختار عدداً عشوائياً n من الكبر المناسب حتى يكون مخرج الخوارزمية "احتمال n أولي". عند التطبيق العملي، من الممكن اختبار قابلية قسمة n على أعداد أولية صغيرة ومن الممكن أيضاً فرض شروط أخرى وذلك يعتمد على الغرض من التطبيق.

تمارين

(١١,٣,٥) افرض أن n عدد صحيح فردي مؤلف وأن $1 \leq a < n$. إذا كان $a^{n-1} \not\equiv 1 (\operatorname{mod} n)$ فنقول إن a شاهد فيرما على أن n مؤلف (Fermat witness to compositeness of n). إذا كان a شاهد فيرما على أن n مؤلف فأثبت أن a شاهد أويلر على أن n مؤلف.

(١١,٣,٦) نفذ اختبار سولوفي وستراسن على العدد $n = 91$. اختار $a = 74$ كأول قيمة "عشوائية" للعدد a. إذا لم تكن سيء الحظ فالاختيار العشوائي الثاني للعدد a سيثبت أن n مؤلف.

(١١,٣,٧) (اختبار ميلر ورابن) ليكن n عدداً صحيحاً فردياً وليكن $n - 1 = 2^s r$ حيث r عدد فردي ولنفرض أن $a \in \mathbb{Z}_n^*$.

حقيقة: إذا كان n عدداً أولياً فإما أن يكون $a^r \equiv 1 (\operatorname{mod} n)$ أو يوجد j، $0 \leq j < s$ بحيث يكون $a^{2^j r} \equiv -1 (\operatorname{mod} n)$.

تعريف: افرض أن n مؤلف. إذا كان $a^r \not\equiv 1 (\operatorname{mod} n)$ وكان $a^{2^j r} \not\equiv -1 (\operatorname{mod} n)$ لكل j، $0 \leq j < s$ فنقول إن a شاهد قوي على أن n مؤلف (Strong witness to compositeness of n).

حقيقة: إذا كان $n \neq 9$ عدداً فردياً مؤلفاً فعدد الشواهد القوية $a \in \mathbb{Z}_n^*$ على أن n مؤلف يزيد عن ثلاثة أرباع عناصر $\mathbb{Z}_n^*$.

(أ) استخدم المفاهيم والحقائق السابقة لتصميم اختبار لأولية العدد n.
(ب) ما هو الزمن اللازم (عدد العمليات الثنائية) لتنفيذ الخوارزمية.
(ج) ناقش صواب النتائج التي تحصل عليها من هذا الاختبار.

(١١,٤) التحليل والجذور التربيعية
Factoring and Square Roots

إن مسألة كتابة عدد مؤلف n كحاصل ضرب عوامله الأولية تعدت كونها مسألة أكاديمية فقط حيث عديد من أنظمة التعمية ذات الانتشار الواسع (مثل نظام RSA الذي نقدمه في الفصل الثاني عشر) تعتمد تماماً على صعوبة تحليل عدد مؤلف n. من المؤكد أن تحليل مثل هذا العدد سيؤدي إلى شهرة من ينجح بذلك:

خصصت صحيفة نيوورك تايمز في العام ١٩٨٨م الصفحة الأولى عن استخدام طريقة المرشح التربيعي (نناقشه في البند (**١١,٤,٢**)) لتحليل عدد مكون من 100 مرتبة بالاستعانة بشبكة حاسبات مؤلفة من 400 حاسب.

لا توجد لحد الآن خوارزمية فعالة لتحليل عدد n دون وضع قيود عليه، ولكن توجد بعض الخوارزميات الفعالة عند وضع شروط مقيدة على n. على سبيل المثال، من الممكن تجريب القسمة على أعداد أولية للحصول على عامل صغير، كما أن طريقة بولارد رو (التي سنقدمها لاحقاً) هي طريقة فعالة للحصول على قواسم صغيرة نسبياً للعدد n. التحدي الذي ناقشه مقال مجلة نيوورك تايمز يتعلق بالعدد $n = pq$ حيث p و q عددان أوليان مكونان من 41 و 60 مرتبة على التوالي وتم اختيارهما بعناية لاختبار خوارزمية مصممة لأغراض خاصة. وفي مثل هذه الحالات تم اختيار خوارزمية عامة من عائلة المربعات العشوائية[١].

---

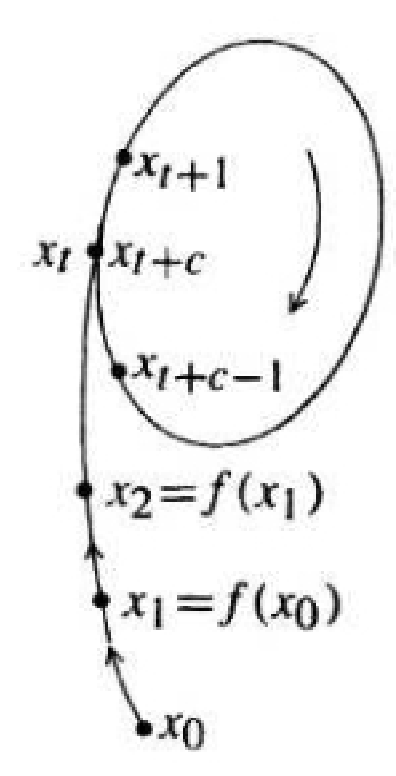
(١) في الثاني عشر من أكتوبر ١٩٨٨م كتب مالكم براوني "التغلب على مسألة رياضية شديدة الصعوبة". ولكن براوني كان أقل حماسة من محرري مجلة نيوورك تايم حيث كتبوا العنوان الدراماتيكي "تم التغلب على أصعب مسألة رياضية باستخدام مئات الحاسبات".

فيما يلي نفترض أن للعدد n على الأقل قاسمين أوليين مختلفين ؛ لأن العدد الذي يكون على الصورة $n = x^k$ حيث $x \in \mathbb{Z}$ و $k > 1$ يسهل التعرف عليه ومن ثم يسهل الحصول على قاسم غير تافه (تمرين (**١١,٤,٩**)).

(١١,٤,١) طريقة رو لبولارد

لدينا المسألة التالية: نفرض أن X مجموعة منتهية وأن $f : X \to X$ وأن $x_0 \in X$. من الممكن تعريف المتتالية $(x_i) \subseteq X$ على النحو التالي: $x_1 = f(x_0)$ ، $x_2 = f(x_1)$ وهكذا. أي أن $x_i = f(x_{i-1})$ لكل عدد صحيح موجب i. بما أن X منتهية فحدود المتتالية ستتكرر بعد قيمة معينة. أي يوجد $i < j$ بحيث يكون $x_i = x_j$. والمسألة هي إيجاد هذا الزوج (i, j).

للمساعدة على فهم هذه المسألة نقوم بإنشاء شكل رو (rho-diagram) للمتتالية f ببذرة x_0 (انظر الشكل أدناه).



يبين الشكل الرؤوس x_i لجميع قيم x_i المختلفة ويوجد ضلع موجه من x_i إلى $x_{i+1} = f(x_i)$ لكل i. جاءت تسمية الشكل من كونه يشبه حرف الهجائية اليونانية ρ.

لنفرض أن c هو عدد الأضلاع الموجهة في دورة الشكل وأن t هو عدد الأضلاع الموجهة في ذيل الشكل. ولذا فعدد الأضلاع الموجهة في الشكل يساوي $k = t + c$

حيث k عدد الرؤوس. الرأس الذي يلتقي عنده الذيل بالدورة هو $x_t = x_{t+c}$. لاحظ أنه إذا كان i و j عددين صحيحين غير سالبين فيكون $x_i = x_j$ إذا وفقط إذا كان $i = j$ أو $i \equiv j (\bmod c)$ في حالة $t \leq i$ و $t \leq j$.

إحدى الطرق لحل هذه المسألة هي حساب x_i بالتتالي وتخزينها ثم مقارنة كل x_i جديدة مع جميع القيم التي تم تخزينها إلى أن نحصل على المساواة المطلوبة. ولكن هذه الطريقة تحتاج إلى تخزين جميع قيم x_i (عددها k) في شكل رو، وبهذا فهي طريقة غير عملية؛ لأن k عادة ما يكون كبير جداً. وأما إذا اتبعنا طريقة رو لبولارد فنحتاج فقط إلى تخزين متغيرين x و y. نبدأ أولاً بوضع $x = x_0$ و $y = y_0$. ثم نكرر حساب:

$$x \leftarrow f(x) \quad \text{و} \quad y \leftarrow f(f(y))$$

(أي أننا نستبدل x بالمقدار $f(x)$ ونستبدل y بالمقدار $(f(f(y)))$ إلى أن نحصل على $x = y$. بعد الخطوة i يكون $x = x_i$ و $y = x_{2i}$. إذا توقفت الطريقة بعد الخطوة m حيث:

$$x_m = x = y = x_{2m}$$

فيكون الزوج المرتب $(m,2m)$ هو الحل المنشود لمسألتنا.

من السهل إثبات أن m هو أصغر عدد صحيح موجب يحقق $m \geq t$ و $c \mid m$. تتوقف هذه الطريقة بعد $m < k$ من الخطوات وتستخدم عدد $3m < 3k$ من العمليات على f. إذا كانت f عشوائية وكان $n = \left|X\right|$ عدداً كبيراً فمن الممكن إثبات أن كل من t و c يساوي تقريباً $\sqrt{\pi n / 8}$. ومن ثم $k = c + t$ يساوي تقريباً $\sqrt{\pi n / 2} \approx 1.253\sqrt{n}$.[٢]

---

(٢) تقدير k يرتبط مع محيرة تاريخ الولادة: إذا كان لدينا مجموعة أشخاص عددها 23 فإن احتمال أن يكون تاريخ ميلاد شخصان منهم على الأقل في اليوم نفسه يساوي $\frac{1}{2}$ على الأقل. إن مثل هذا الاعتبار شائع الاستخدام في الخطط المصممة للهجوم التي تعتمد على تقصي عشوائي لإيجاد تضاربات تؤدي إلى "جذر تربيعي" للحدود الدنيا على عدد عناصر مجموعات معينة (تعرف هذه الطريقة بهجوم تاريخ الولادة).

نعـود الآن إلى مسـألة تحليـل عـدد مؤلـف معطـى n لنفـرض أن $p < \sqrt{n}$ قاسـم أولـي (غـير معلـوم) للعـدد n. هـدفنا هـو إيجـاد عـددين صـحيحين x و y حيـث $x \equiv y (\bmod p)$ ولكن $x \not\equiv y (\bmod n)$. عندئذ، يكون $d = (x - y, n)$ قاسماً غير تافه للعدد n. إذا كـان d أو $\frac{n}{d}$ مؤلفاً فنكـرر العمليـة إلى أن نحصـل علـى قاسـم أولـي للعدد n.

الفكرة الأساسية هنا هي تنفيذ طريقة رو على دالة f معرفة على $\mathbb{Z}_n$ مع التظاهر على أن خطوات التنفيذ تتم على $\mathbb{Z}_p$ مع أن p غير معلوم. ولكي نضمن نجاح هذا التظاهر فيجب أن تحقق f الخاصية التالية:

لكل $a, b \in \mathbb{Z}_n$، إذا كان $a \equiv b (\bmod p)$ فإن $f(a) \equiv f(b) (\bmod p)$. كثيرات الحدود تحقق هذه الخاصية، ولذا يكون من المناسب اختيار f على أنها كثيرة حدود. ومن المستحسن أن تشابه f دالة معرفة على $\mathbb{Z}_p$، وذلك لتحسين فرص النجاح. إحدى هذه الدوال هي $f(x) = x^2 + 1$ حيث البذرة $x_0 = 2$ (من الممكن اختيار دالة أخرى ولكن بالتأكيد ليست دالة خطية).

وبهذا تكون تفاصيل الطريقة على النحو التالي لكثيرة حدود f بمعاملات صحيحة و $x_0 \in \mathbb{Z}_n$: نبدأ بوضع $x = x_0$ و $y = y_0$ ونكرر الخطوتين:

$$x \leftarrow f(x) (\bmod n)$$
$$y \leftarrow f(f(y)) (\bmod n)$$

إلى أن نحصل على $d = (x - y, n) > 1$. إذا كان $d < n$ فنكون قد نجحنا في تحليل n. أما إذا كان $d = n$ فالطريقة تفشل وفي هـذه الحـالة نجرب دالة أخـرى f وبذرة أخرى x_0.

بما أن $p \leq \sqrt{n}$ فمن المتوقع أن يكون الزمن اللازم لحساب f هو على الأكثر $3\sqrt{\pi p / 2} = O(\sqrt{p}) = O(n^{1/4})$. ومع أن هذه الطريقة لا تعدُّ فعالة من الناحية

النظرية، إلا أنها أفضل من تجريب جميع d حيث $1 < d \le \sqrt{n}$ لنرى فيما إذا كان $d \mid n$ ، حيث الزمن الذي تحتاجه هذه الطريقة يساوي $O\left(n^{1/2}\right)$ عملية قسمة.

وكمثال، دعنا نستخدم طريقة رو لتحليل $n = 551$ حيث $f(x) = x^2 + 1 (\bmod 551)$ و $x_0 = 2$. الجدول التالي يبين خطوات حساب x ، y ، $d = (x - y, n)$.

$x \leftarrow f(x)$	$y \leftarrow f(f(y))$	$d = (x - y, 551)$
5	26	1
26	449	1
126	240	19

لاحظ أن كلا العددين 19 و $29 = \frac{551}{19}$ هو عدد أولي . وبهذا نكون قد حصلنا على تحليل العدد $551 = 19 \cdot 29$.

(١١,٤,٢) المربعات العشوائية

من أفضل طرق تحليل أعداد عامة هي عائلة المربعات العشوائية حيث استخدمت طريقة المرشح التربيعي (quadratic sieve) في العام ١٩٩٤م لتحليل أعداد عدد مراتبها العشرية بين 100 إلى 129 مرتبة. واستخدمت طريقة أكثر تعقيداً من هذه العائلة تدعى مرشح الحقل العددي (number field sieve) في العام ١٩٩٦م لتحليل عدد مكون من 130 مرتبة عشرية، وفي العام ١٩٩٩م لتحليل عددين عدد مراتبهما العشرية هو 140 و 155 مرتبة، وهذه الأعداد هي الأعداد التي اقترحتها مختبرات RSA. والتي أطلق عليها تحدي RSA.

لنفرض أن n عدد مؤلف. المطلوب هنا هو إيجاد $x, y \in \mathbb{Z}_n$ حيث $x^2 \equiv y^2 (\bmod n)$. فإذا كان $x \not\equiv \pm y (\bmod n)$ فإن $(x + y, n)$ هو قاسم غير تافه للعدد n ؛ لأن n يقسم $x^2 - y^2 = (x - y)(x + y)$ ولكن n لا يقسم أي من العددين

$x - y$ و $x + y$. وكحالة خاصة، إذا كان $n = pq$ حيث p و q عددان أوليان مختلفان فعندئذ يكون عدد حلول التطابق $x^2 \equiv a^2 (\bmod n)$ يساوي أربعة حلول ($a \in \mathbb{Z}_n^*$ معطى) ويمكن إيجاد هذه الحلول باستخدام مبرهنة الباقي الصينية. على سبيل المثال، إذا كان $n = 15$ واستطعنا بطريقة أو بأخرى الحصول على $x = 2$ و $y = 7$ تحقق التطابق $x^2 \equiv y^2 (\bmod 15)$ فنجد أن $(x + y, n) = (9, 15) = 3$ وهذا قاسم غير تافه للعدد 15.

إحدى الطرق المتبعة لإيجاد x و y مناسبين هي حساب مجموعة الأزواج المرتبة $\left(a_i, b_i \equiv a_i^2 (\bmod n)\right)$ حيث a_i عدد عشوائي ومحاولة إيجاد مجموعة جزئية S بحيث يكون $\prod_{i \in S} b_i$ مربعاً كاملاً. في هذه الحالة، $x = \prod_{i \in S} a_i$ والجذر التربيعي y للعدد $\prod_{i \in S} b_i$ يحققان $x^2 \equiv y^2 (\bmod n)$. وإضافة إلى ذلك، إذا كان $x \not\equiv \pm y (\bmod n)$ فنكون قد نجحنا في تحليل n ، وإذا كان $x \equiv \pm y (\bmod n)$ فنقوم باختيار مجموعة S مختلفة (من الممكن أن نحتاج لتوليد المزيد من الأزواج المرتبة $\left(a_i, b_i\right)$).

بصورة أدق نقوم باختيار أساس للتحليل $B = \{p_1, p_2, \ldots, p_t\}$ تحتوي على أول t من الأعداد الأولية. إذا استطعنا تحليل b على B فنأخذ الزوج المرتب $\left(a, b \equiv a^2 (\bmod n)\right)$ ويسمى b في هذه الحالة عدد ناعم من النوع p_t (p_t-smooth). لنفرض أننا حصلنا على الأزواج المرتبة $\left(a_i, b_i\right)$ حيث $b_i = \prod_{j=1}^{t} p_j^{e_{ij}}$ ، $1 \le i \le t + 1$ هو تحليل b_i . الآن، نقوم باختيار المجموعة S بحيث تظهر القوى الزوجية فقط للأعداد الأولية في العدد $\prod_{i \in S} b_i$. لاحظ أن أي $t + 1$ متجهاً $e_i = \left(e_{i1}, \ldots, e_{it}\right) (\bmod 2)$ يجب أن تكون مرتبطة خطياً على $\mathbb{Z}_2$ وتوجد مجموعة S يكون $\sum_{i \in S} e_i$ هو المتجه الصفري. عندئذ، يكون العدد $\prod_{i \in S} b_i$ على الشكل المطلوب.

مثال (١١,٤,١)

نوظف الطريقة لتحليل $n = 10057$. لنفرض أن $t = 5$. عندئذ، أساس التحليل هو المجموعة $B = \{2,3,5,7,11\}$ الجدول التالي يبين خيارات a_i حيث يحتفظ فقط بالخيارات التي تؤدي إلى تحليل $b_i \equiv a_i^2$ على أساس التحليل.

i	a_i	$b_i \equiv a_i^2 (\bmod n)$	التحليل
1	7231	1018	$2 \cdot 509$
1	105	968	$2^3 \cdot 11^2$
2	115	3168	$2^5 \cdot 3^2 \cdot 11$
3	1006	6336	$2^6 \cdot 3^2 \cdot 11$
4	3010	8800	$2^5 \cdot 5^2 \cdot 11$
5	4014	882	$2 \cdot 3^2 \cdot 7^2$
6	4023	2816	$2^8 \cdot 11$

لاحظ إهمال الخيار $a = 7231$ ؛ لأن $a^2 (\bmod n)$ لا يتحلل تماماً على أساس التحليل. وفي هذه الحالة التحليل المقابل في العمود الأخير هو فقط تحليل جزئي.

يوجد عدد $t + 1 = 6$ من الأزواج المرتبة (a_i, b_i). ومن ثم توجد مجموعة S بحيث يكون $\prod_{i \in S} b_i$ مربعاً كاملاً. وبالتجريب نجد أن $S = \{4,5,6\}$ تؤدي إلى $x^2 \equiv y^2 (\bmod n)$ حيث $x = 3010 \cdot 4014 \cdot 4023 \equiv 2748 (\bmod n)$ و $y = 2^7 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \equiv 7042 (\bmod n)$. وبما أن $x \not\equiv \pm y (\bmod n)$ فنحصل على القاسم غير التافه $(x + y, n) = 89$ ويكون $n = 10057 = 89 \cdot 113$.

من الممكن أيضاً الحصول على مربع كامل باختيار $S = \{1,5\}$. والقيم المقابلة لذلك هي $x = 105 \cdot 4014 \equiv 9133 (\bmod n)$ و $y = 2^2 \cdot 3 \cdot 7 \cdot 11 = 924$. ولكن $x \equiv -y (\bmod n)$. وبهذا لا نحصل على معلومات مفيدة من هذا الخيار. ▲

لاحظ أن اختيار أساس تحليل أكبر يزيد من فرصة أن يكون b_i ناعم من النوع p_t ولكن هذا يحتاج إلى المزيد من العلاقات. إذا كان t معطى فإحدى الإستراتيجيات المتبعة لزيادة فرص الحصول على أعداد ناعمة من النوع p_t هي اختيار a بحيث يكون $b \equiv a^2 (\bmod n)$ صغيراً نسبياً. ومثال مشهور على ذلك هي طريقة المرشح التربيعي.

لنفرض أن n معطى وأن $m = \left\lfloor \sqrt{n} \right\rfloor$. نعرف الدالة $q : \mathbb{Z} \to \mathbb{Z}$ بالقاعدة $q(z) = (z+m)^2 - n$. لاحظ أن $q(z) \approx z^2 + 2zm$ وإذا كان $|z|$ صغيراً فإن $|q(z)|$ صغير بالنسبة إلى n. في خوارزمية المرشح التربيعي نضع $a = z + m$ و $b = q(z) = a^2 - n$ حيث $z = 0, \pm 1, \ldots$. بما أنه من الممكن أن يكون b سالباً فإننا نضيف -1 إلى أساس التحليل. إضافة إلى ذلك، لاحظ أنه إذا كن p قاسماً أولياً للعدد b فإن $a^2 \equiv n (\bmod p)$. وبهذا يكون n راسباً تربيعياً قياس p (إلا إذا كان $p \mid n$). ولذا فأساس التحليل يحتاج فقط احتواء الأعداد الأولية p التي تحقق $\left(\frac{n}{p}\right) = 1$.

مثال (١١,٤,٢)

سنحلل العدد $n = 10057$ المقدم في المثال السابق. ضع $m = \left\lfloor \sqrt{n} \right\rfloor = 100$ و $q(z) = (z + 100)^2 - 10057$. لنفرض أن أساس التحليل هو $B = \{2, 3, 11, 19\} \cup \{-1\}$ (B تحتوي على الأعداد الأولية $p \leq 19$ التي تحقق $\left(\frac{n}{p}\right) = 1$). الجدول التالي يبين بعض قيم z التي تجعل $q(z)$ يتحلل على أساس التحليل:

z	$a = z + m$	$b = q(z)$	التحليل
0	100	-57	$-3 \cdot 19$
-1	99	-256	-2^8
1	101	144	$2^4 \cdot 3^2$
-3	97	-648	$-2^3 \cdot 3^4$
5	105	968	$2^3 \cdot 11^2$

مـــن العلاقـــات للعـــدد $z \in \{-1,-3,5\}$ نجـــد أن $x^2 \equiv y^2 (\bmod n)$ حيـــث $x = 99 \cdot 97 \cdot 105$ و $y = 2^7 \cdot 3^2 \cdot 11$. ولكن $x \equiv y (\bmod n)$ في هذه الحالة ومن ثـم فالطريقـة تفشـل في تحليـل n. وإذا اخترنـا $z = 1$ فنجـد أن $101^2 \equiv 2^4 \cdot 3^2$. وبملاحظة أن $x = 101$ و $y = 2^2 \cdot 3$ يحققان $x \not\equiv \pm y (\bmod n)$ فإننا نحصل على قاسم غير تافه $(x + y, n) = 133$ للعدد 10057. ▲

تحتاج عملية اختيار الأزواج المرتبة المناسبة (a,b) إلى جهد كبير، ويستعاض عن طريقة تجريب القواسم بطريقة المرشح الأكثر فعالية لاختبار النعومة. على سبيل المثال، في العام ١٩٩٤م احتاج تحليل العدد المشهور المكون من 129 مرتبة إلى 600 شخص و 1600 آلة للحصول على أكثر من 8 ملايين علاقة خلال سبعة أشهر حيث كان عدد عناصر أساس التحليل يساوي 524339 (انظر [1]). ومنذ العام ١٩٩٩م تبين أن محاولة تحليل عدد مختار جيداً n عدد مراتبه الثنائية يساوي 1024 (308 مرتبة عشرية) هي محاولة مستحيلة حتى مع استخدام طريقة مرشح الحقل العددي المطورة.

(١١,٤,٣) الجذور التربيعية

يبين البند السابق وجود علاقة بين مسألتي التحليل والجذور التربيعية. في الحقيقة هاتان المسألتان متكافئتان وهذا ما سنبينه في هذا البند.

تذكر أن طريقة تحليل المربعات العشوائية تتم بمحاولة إيجاد x و y حيث $x^2 \equiv y^2 (\bmod n)$. فإذا كان $x \not\equiv \pm y (\bmod n)$ فإننا نحصل على قاسم غير تافه $(x + y, n)$ للعدد n. وبهذا يكون من الواضح أننا لو استطعنا إيجاد جميع الجذور التربيعية لراسب تربيعي $x^2 \in \mathbb{Z}_n^*$ فإننا سنحصل على قاسم غير تافه للعدد n. من المعلوم عدم وجود طريقة فعالة عامة لإيجاد الجذور التربيعية ومع ذلك سنناقش ما ستؤديه مثل هذه الخوارزمية.

سندرس الطريقة للمثال $n = pq$ حيث p و q عددان أوليان فرديان مختلفان (يمكن تعميم هذه الطريقة على الحالة العامة). استناداً إلى النتيجة (**١١,٢,٢**) نرى وجود جذران تربيعان بالضبط لراسب تربيعي قياس عدد أولي. ويمكن اللجوء إلى مبرهنة الباقي الصينية لإثبات وجود أربعة جذور تربيعية للتطابق $x^2 \equiv a(\mod pq)$ حيث $a \in Q_{pq}$.

لنفرض الآن وجود خوارزمية يكون مخرجها جذراً تربيعياً للعدد $a \in Q_{pq}$. لتحليل العدد pq ، نقوم باختيار عشوائي لعدد $x \in \mathbb{Z}_n^*$ وإدخال $x^2(\mod n)$ إلى الخوارزمية. لكل من الأعداد المختارة x نجد باحتمال يساري $\frac{1}{2}$ أن $y \not\equiv \pm x(\mod n)$ حيث y هو الجذر التربيعي الناتج عن تنفيذ الخوارزمية. أي من المتوقع الحصول على قاسم غير تافه $(x + y, n)$ للعدد n بمحاولتين فقط.

نقول إن مسألة تحليل n تختزل إلى مسألة إيجاد الجذور التربيعية. وبدقة أكثر، إذا كانت A و B مسألتين حسابيتين فنكتب $A \le B$ ، إذا استطعنا حل المسألة A بزمن حدودي (بدلالة حجم البيانات المدخلة) بوجود خوارزمية حدودية لحل المسألة B . أي أن $A \le B$ تعني أن المسألة A ليست أصعب من المسألة B . ونقول إن المسألتين A و B متكافئتان حسابياً إذا كان $A \le B$ و $B \le A$. ونستخدم المفهوم نفسه في حالة الخوارزميات العشوائية التي تحتاج لزمن تنفيذ حدودي بدلالة سعة المدخلات. على وجه الخصوص FACTOR ≤ SQROOT.

سنبين الآن كيفية إيجاد الجذور التربيعية لراسب تربيعي $a \in Q_n$ إذا علمنا تحليل n (أي سنبرهن أن SQROOT ≤ FACTOR). لنفرض أن لدينا الجذور التربيعية قياس كل من العددين الأوليين p و q . عندئذ، نستطيع إيجاد الجذور التربيعية الأربعة للعدد a قياس $n = pq$ وذلك بإيجاد x و y اللذان يحققان التطابقات:

$$\begin{Bmatrix} x \equiv a_p(\mod p) \\ x \equiv a_q(\mod q) \end{Bmatrix} \quad \text{و} \quad \begin{Bmatrix} y \equiv -a_p(\mod p) \\ y \equiv a_q(\mod q) \end{Bmatrix}$$

حيث a_r هو جذر تربيعي للعدد a قياس r. عندئذ، الجذور الأربعة هي $\pm x$ و $\pm y$. وبهذا نكون قد وجدنا خوارزمية فعالة لمسألة SQROOT على فرض وجود خوارزمية فعالة لإيجاد الجذور التربيعية قياس عدد أولي.

لنفرض أولاً الحالة التي يكون فيها العدد الأولي p على الصورة $p \equiv 3 (\bmod 4)$. عندئذ، استناداً إلى معيار أويلر نجد أن:

$$a^{(p-1)/2} \equiv 1 (\bmod p)$$

حيث $a \in Q_p$. ومن ثم فإن:

$$\left(a^{(p+1)/4}\right)^2 \equiv a^{(p+1)/2} \equiv a^{(p-1)/2} a \equiv a (\bmod p)$$

إذن، الجذران التربيعيان للعدد a قياس العدد p هما $\pm a^{(p+1)/4}$. الآن، إذا كان كل من العددين الأوليين p و q على الصورة $4k + 3$ (يسمى العدد $n = pq$ في هذه الحالة، عدد بلم Blum integer) فنكون قد وجدنا خوارزمية فعالة لإيجاد الجذور التربيعية للعدد a قياس n.

في الحقيقة، توجد خوارزمية سهلة نسبياً لإيجاد الجذور التربيعية قياس عدد أولي إذا علمنا راسب غير تربيعي (على وجه الخصوص، إذا كان $p \equiv 5 (\bmod 8)$ فإن $2 \in \overline{Q_p}$، انظر [63]). ولكن لا توجد خوارزمية فعالة غير احتمالية لإيجاد راسب غير تربيعي قياس عدد أولي. وبما أن نصف عناصر $\mathbb{Z}_p^*$ هي رواسب غير تربيعية فتوجد خوارزمية فعالة احتمالية لإيجاد الجذور التربيعية قياس عدد أولي وذلك باختيار أعداد عشوائية x حتى الحصول على عدد يحقق $\left(\frac{x}{p}\right) = -1$.

مما سبق نستطيع ضمان طرق فعالة لإيجاد الجذور التربيعية قياس عدد أولي. وبهذا يكون SQROOT$\leq$FACTOR ونخلص إلى تكافؤ المسألتين حسابياً. سنناقش ذلك لاحقاً في البند (١٢،٣) مرة أخرى عند دراستنا لبرهان أمن أنظمة التعمية.

تمارين

(**١١,٤,٣**) يوضح هذا التمرين طريقة رو لبولارد لتحليل العدد $n = 391 = 17 \cdot 23$:

(أ) نفذ طريقة رو لبولارد حيث $x_0 = 2$ و $x_{i+1} = f(x_i) = x_i^2 + 1(\bmod n)$

(تذكر أن الخوارزمية تتوقف عندما يكون $1 < (x_{2i} - x_i, n) < n$. سنحصل على قاسم غير تافه عندما يكون $i = 4$).

(ب) أكمل الجدول التالي :

i	0	1	2	3	4	5	6	7	8
$x_i(\bmod 17)$	2	5	9	14	10	16	2		
$x_i(\bmod 23)$	2								

ارسم مخطط رو لكل صف من صفوف الجدول موضحاً الذيل والدورة.

(ج) بين كيفية اختيار عدد مؤلف n يؤدي إلى فشل طريقة رو لبولارد لتحليل هذا العدد.

(**١١,٤,٤**) حلل العدد $n = 5141$ بطريقة رو لبولارد مستخدماً $x_0 = 1$ و $x_{i+1} \equiv x_i^2 + 2(\bmod n)$ ، $i \geq 0$.

(**١١,٤,٥**) حلل العدد $n = 1081$ بطريقة المرشح التربيعي (كما في المثال (**١١,٤,٢**)) مستخدماً أساس تحليل مناسب يحتوي على جميع الأعداد الصحيحة التي لا يزيد عن العدد 11.

(**١١,٤,٦**) حلل العدد $n = 24961$ بطريقة المرشح التربيعي (كما في المثال (**١١,٤,٢**)) مستخدماً أساس تحليل مناسب يحتوي على جميع الأعداد الصحيحة التي لا تزيد عن العدد 23.

(**١١,٤,٧**) إذا كان $n = ab$ حيث $|a - b|$ صغير نسبياً فمن الممكن تحليل العدد بخطوات قليلة باستخدام طريقة فيرما للتحليل التي يمكن وصفها على النحو التالي :

- لنفرض أن n عدد فردي. يوجد تقابل بين تحليل n على الصورة $n = ab$ حيث $0 < a \leq b$ والتمثيل $n = t^2 - s^2$ حيث t و s عددان صحيحان غير سالبين. هذا التقابل هو:

$$ab = t^2 - s^2 = (t-s)(t+s)$$

حيث $t = \frac{a+b}{2}$ و $s = \frac{a-b}{2}$.

- إذا كان العددان a و b قريبان من بعضهما فإن $s = \frac{a-b}{2}$ عدد صغير ويكون $t \approx \sqrt{n}$.
- لتحليل n ، نقوم بتجريب قيم متتالية للعدد t مبتدئين بالقيمة $\lceil \sqrt{n} \rceil$ حتى نحصل على مربع كامل $t^2 - n$.

حلل العدد $n = 2881$ بطريقة فيرما للتحليل. لمعرفة تفاصيل طريقة فيرما للتحليل (انظر [50]و [74]).

(**١١,٤,٨**) بين كيفية الحصول على الجذور التربيعية للعدد $179 \in \mathbb{Z}_{187}$ مستخدماً التحليل $187 = 11 \cdot 17$.

(**١١,٤,٩**) صمم اختبار فعال لمعرفة فيما إذا كان n قوة كاملة (أي أن $n = x^k$ حيث x عدد صحيح و $k > 1$). إذا كان n قوة كاملة فجد تحليل جزئي للعدد n.

(**١١,٤,١٠**) لنفرض أن $n = pq$ حيث $p \neq q$ عددان أوليان ولنفرض أن $\varphi = \varphi(n) = (p-1)(q-1)$. مسألة حساب φ يرمز لها بالرمز COMPUTE Φ وهي مسألة إيجاد φ بمعرفة n. صمم خوارزمية فعالة لمسألة FACTOR بمعرفة خوارزمية لحساب COMPUTE Φ.

(١١,٥) اللوغاريتمات المنفصلة

Discrete Logarithms

لنفرض أن p عدد أولي فردي وأن α مولداً للزمرة $\mathbb{Z}_p^*$. لنفرض أن $\beta \in \mathbb{Z}_p^*$. اللوغاريتم المنفصل للعدد β للأساس α (the discrete logarithm of β to the base α) ويكتب $\log_\alpha \beta$ هو العدد الصحيح الوحيد x حيث $0 \le x \le p-2$ الذي يحقق $\beta \equiv \alpha^x (\bmod n)$. على سبيل المثال، $\alpha = 3$ مولداً للزمرة $\mathbb{Z}_5^*$ وأن $\log_3 4 = 2$ لأن $4 \equiv 3^2 (\bmod 5)$.

مسألة اللوغاريتيم المنفصل أو اختصاراً DLP تنص على:

جد x إذا علمت (p, α, β).

كما هو الحال في مسألة تحليل العدد فإن مسألة اللوغاريتم المنفصل مسألة تافهة من الناحية النظرية وذلك بالقيام بحساب α^x بتجريب قيم $x \ge 0$ حتى نجد β. ولكن هذه الطريقة غير فعالة؛ لأنها تحتاج إلى $O(p)$ عملية ضرب قياس p. لا توجد خوارزمية فعالة لحساب مسألة اللوغاريتم المنفصل ولهذا يعتمد أمن العديد من أنظمة التعمية على فرضية عدم وجود خوارزمية فعالة لحل مسألة DLP. سنقدم هنا خوارزميتان لحساب DLP وكلاهما ليست حدودية ولكنهما أفضل من طريقة الاستنفاد.

(١١,٥,١) الخطوة الصغيرة والخطوة الكبيرة

تشبه خوارزمية الخطوة الصغيرة والخطوة الكبيرة إلى حد ما هجوم اللقاء في المنتصف على النظام DES المضاعف حيث يكون عدد عمليات الضرب قياس العدد أصغر من عدد العمليات باستخدام طريقة الاستنفاد ولكن ذلك يكون على حساب سعة التخزين اللازمة.

لنفرض أن $m = \left\lceil \sqrt{p-1} \right\rceil$. إذا كان $\beta \equiv \alpha^x (\bmod p)$ فحينئذ نكتب $x = im + j$ حيث $0 \le i, j < m$ و $\beta \equiv \alpha^x \equiv \alpha^{im}\alpha^j$ أو $\beta\alpha^{-im} \equiv \alpha^j$. نشكل الآن جدولاً مدخلاته $\left(j, \alpha^j (\bmod p)\right)$ حيث $0 \le j < m$. لكل i،

$0 \le i < m$. نقوم بحساب $\beta\alpha^{-im} (\bmod p)$ ونبحث عن قيمة مساوية لهذا العدد في الجدول. وعند وجود هذه القيمة يكون لدينا:

$$\beta\alpha^{-im} \equiv \alpha^j (\bmod p).$$

ومن ثم نحصل على:

$$\log_\alpha \beta = im + j.$$

مثال (١١,٥,١)

لنفرض أن $p = 41$ ، $\alpha = 6$ ، $\beta = 2$. سنقوم بتطبيق الخوارزمية لحساب $\log_6 2 \in \mathbb{Z}_{41}$.

بوضع $m = \lceil \sqrt{40} \rceil = 7$ وإنشاء جدول مدخلاته (j, α^j) حيث $0 \le j < 7$ نحصل على:

j	0	1	2	3	4	5	6
$\alpha^j (\bmod p)$	1	6	36	11	25	27	39

عندئذ، $\alpha^{-1} \equiv 7 (\bmod p)$ و $\alpha^{-m} \equiv 7^7 \equiv 17 (\bmod 41)$. الآن، نقوم بحساب $\beta(\alpha^{-m})^i (\bmod p)$ حتى نحصل على المدخل المطلوب:

$$\begin{aligned} i = 0 &: \quad \beta\left(\alpha^{-m}\right)^0 \equiv \beta \equiv 2 \\ i = 1 &: \quad \beta\left(\alpha^{-m}\right)^1 \equiv 2 \cdot 17 \equiv 34 \\ i = 2 &: \quad \beta\left(\alpha^{-m}\right)^2 \equiv 34 \cdot 17 \equiv 4 \\ i = 3 &: \quad \beta\left(\alpha^{-m}\right)^3 \equiv 4 \cdot 17 \equiv 27 \end{aligned}$$

وبهذا نحصل على قيمة من قيم الجدول عند $i = 3$ و $j = 5$ مما يؤدي إلى أن $\beta\alpha^{-3m} = \alpha^5$. أي أن $\beta \equiv \alpha^{21+5} (\bmod p)$ ويكون $\log_6 2 = 26 \in \mathbb{Z}_{41}$. ▲

يحتاج إنشاء الجدول إلى عدد $m - 1$ من عمليات الضرب قياس عدد. والخطوة الكبيرة تحتاج إلى أخذ المعكوس وعدد $O(m)$ من عمليات الضرب قياس عدد. ولذا

فالزمن اللازم لتنفيذ الخوارزمية يحتاج إلى $O\left(\sqrt{p-1}\right)$ من عمليات الضرب قياس عدد، وهذا أفضل من طريقة الاستنفاد ولكنه أسوأ بكثير من زمن حدودي.

(١١,٥,٢) حساب الدليل

إن أفضل الطرق لحساب اللوغاريتم المنفصل هي طرق معدلة من خوارزمية حساب الدليل وبعض من هذه الطرق يشبه خوارزميات المربعات العشوائية للتحليل. الخطوة الحسابية الأولى (غالية التكاليف) تجد لوغاريتمات عناصر أساس تحليل مختار B (ليس بالضرورة أن يعتمد على أعداد معينة β لحساب $\log_\alpha \beta$). أما الخطوة الثانية فتجد لنا عدد صحيح k حيث $\alpha^k\beta$ يتحلل على B. وبحالة نجاح الخطوتين يكون $\log_\alpha \beta$ سهل الحساب.

نقوم باختيار أساس التحليل $B=\{p_1,\ldots,p_t\}$ المكون من أول t عدد أولي. ولنفرض أن الحسابات هي قياس العدد الأولي p. في الخطوة الأولى نقوم باختيار أعداد عشوائية k لمحاولة إيجاد قيم $\alpha^k(\operatorname{mod} p)$ بحيث تتحلل على B. وبهذا يكون:

$$\alpha^k(\operatorname{mod} p) = p_1^{e_1}\ldots p_t^{e_t} \quad \text{حيث} \quad e_i \ge 0 .$$

ومن ذلك نجد أن:

$$k \equiv e_1 \log_\alpha p_1 + \ldots + e_t \log_\alpha p_i (\operatorname{mod} p-1)$$

عادة نجد أكثر من t من هذه التطابقات على أمل نحصل على نظام معادلات خطية في المتغيرات $\log_\alpha p_i$ يكون له حل وحيد.

في الخطوة الثانية نبحث عن قيمة k بحيث يتحلل $\alpha^k\beta(\operatorname{mod} p)$ على B. وإذا نجحنا في ذلك يكون $\alpha^k\beta(\operatorname{mod} p) = p_1^{e_1}\ldots p_t^{e_t}$ حيث $e_i \ge 0$. ومن ذلك نرى أن:

$$k + \log_\alpha \beta \equiv e_1 \log_\alpha p_1 + \cdots + e_t \log_\alpha p_t (\operatorname{mod} p-1)$$

ويكون:

$$\log_\alpha \beta = \left(e_1 \log_\alpha p_1 + \cdots + e_t \log_\alpha p_t - k\right)(\operatorname{mod} p-1) .$$

مثال (١١,٥,٢)

لنفرض أن $p = 19$ ، $\alpha = 2$. سنجد $\log_\alpha 17$. لنفرض أن أساس التحليل هو $B = \{2,3,5\}$. في هذا المثال، $\alpha \in B$ ونحصل مباشرة على $\log_\alpha 2 = 1$. لإيجاد لوغاريتمات العنصرين الآخرين من عناصر B نقوم بحساب $\alpha^k (\bmod p)$ لعدد عشوائي k بحيث نحصل على قيمتين على الأقل كل منهما تتحلل على B :

$$2^9 (\bmod p) = 2 \times 3^2$$
$$2^7 (\bmod p) = 14$$
$$2^{11} (\bmod p) = 3 \times 5$$

يهمل السطر الثاني ؛ لأن 14 لا يتحلل على B . ومن ذلك نحصل على نظام التطابقات :

$$9 \equiv \log_\alpha 2 + 2\log_\alpha 3 (\bmod p-1)$$
$$11 \equiv \log_\alpha 3 + \log_\alpha 5 (\bmod p-1)$$

في المجهولين $\log_\alpha 3$ و $\log_\alpha 5$.

هذا النظام له أكثر من حل. ولذا فمن الممكن أن نحصل على إجابات خاطئة مثل $\log_\alpha 3 = 4$ و $\log_\alpha 5 = 7$. لهذا نقوم بإضافة علاقة أخرى مثل $\alpha^{14} (\bmod p) = 6$ لنحصل على تطابق جديد $14 \equiv \log_\alpha 2 + \log_\alpha 3 (\bmod p-1)$. ومن ثم يكون للنظام الجديد حل وحيد هو :

$$\log_\alpha 3 = 13 \text{ و } \log_\alpha 5 = 16 .$$

الآن ، لإيجاد $\log_\alpha 17$ نبحث عن k بحيث يتحلل $\alpha^k \times 17 (\bmod p)$ على B . على سبيل المثال ، إذا كان $k = 5$ فنجد أن $\alpha^5 \times 17 (\bmod p) = 2^2 \cdot 3$. وبهذا يكون :

$$\log_\alpha 17 \equiv \left(2\log_\alpha 2 + \log_\alpha 3 - 5\right) \equiv 10 (\bmod p-1) . \qquad \blacktriangle$$

إن عملية حساب اللوغاريتمات لعناصر أساس التحليل مكلفة جداً على الرغم من إمكانية توزيع عمليات إيجاد العلاقات المناسبة. يمكن استخدام نتائج الخطوة الأولى

لحساب لوغاريتم أي β معطى بعد إيجاد قيمة k يتحلل $\alpha^k\beta$ على أساس التحليل. إن اختيار أساس تحليل أكبر يسمح بتمثيل عناصر أكثر من $\mathbb{Z}_p^*$ كحاصل ضرب عناصر B ولكن هذا يؤدي إلى حل نظام تطابقات أكبر.

استخدمت هذه الطريقة في العام ١٩٩٠م لحساب لوغاريتمات قياس أعداد أولية عدد مراتبها يقع بين 50 و 100 مرتبة عشرية. على سبيل المثال، قام كل من لاماتشايا (La Macchia) وأدليكو (Odlyzko) (انظر [54]) في العام ١٩٩٠م بحساب لوغاريتمات قياس عدد أولي مكون من 192 مرتبة ثنائية (58 مرتبة عشرية) بزمن معقول باستخدام طريقة معدلة لحساب الدليل تعرف بطريقة أعداد جاوس الصحيحة حيث استطاعوا باختصار نظام مكون من 288017 علاقة بعدد من المجاهيل يساوي 96321 إلى نظام مكون من 7262 علاقة وعدد من المجاهيل يساوي 6006 ومن ثم حل هذا النظام. ثم استخدمت هذه البيانات لحساب لوغاريتمات معينة بجهد بسيط نسبياً. كان لهذا الجهد أهمية عملية حيث يعتمد أمن خطط إثبات الهوية المقترح من قبل أنظمة الميكرو على صعوبة حل مسألة اللوغاريتمات المنفصلة قياس عدد أولي (انظر [88]).

قام كل من جو (Joux) وليرسير (Lercier) في العام ١٩٩٨م بحساب لوغاريتمات منفصلة في الزمرة $\mathbb{Z}_p^*$ حيث p عدد أولي مكون من 90 مرتبة باستخدام طريقة أعداد جاوس الصحيحة مستخدمين لهذا الغرض شبكة مكونة من أربعة حاسبات استطاعت خلال شهر واحد من الحصول على 6٫7 مليون معادلة ومن ذلك حصلوا على 976062 معادلة ظهر فيها كل من المتغيرات على الأقل مرتين. بعد ذلك استطاعوا خلال ثلاثة أسابيع من اختصار النظام الخطي وحله. احتاج حساب لوغاريتمات مختارة إلى 9 ساعات في المتوسط باستخدام حاسب آلي واحد.

لقد استخدم مرشح الحقل العددي لتحليل الأعداد في حساب مسألة اللوغاريتمات المنفصلة، حيث استخدم كل من جو وليرسر في العام ١٩٩٩م طريقة مرشح معدلة

لحساب لوغاريتمات في الزمرة $\mathbb{Z}_p^*$ حيث عدد مراتب p يساوي 100. استخدموا لذلك حاسب آلي من نوع بنتيوم Π جمعت خلال ثمانية شهور $2 \cdot 8$ مليون معادلة ثم استخدموا بعد ذلك معالج (DES Alpha 500 MHZ) لحل نظام المعادلات الخطي خلال ثلاثة أسابيع. احتاج حساب لوغاريتمات مختارة إلى يوم واحد. وبهذا استنتجوا أن طريقة مرشح الحقل العددي أفضل من طريقة أعداد جاوس الصحيحة لحساب اللوغاريتمات المنفصلة قياس أعداد أولية مكونة من أكثر من 100 مرتبة (انظر [46]).

تمارين

(**١١,٥,٣**) إذا علمت أن $\alpha = 5$ مولِّداً للزمرة $\mathbb{Z}_{97}^*$ فاستخدم طريقة الخطوة الصغيرة والخطوة الكبيرة لحساب $\log_5 4 \in \mathbb{Z}_{97}$.

(**١١,٥,٤**) لنفرض أن $p = 41$ وأن $\alpha = 6$ مولِّداً للزمرة $\mathbb{Z}_p^*$. وضح طريقة حساب الدليل لحساب $\log_6 13$ وذلك بإكمال الخطوات التالية:

(أ) اختار $B = \{2,3,5\}$ أساساً للتحليل. افرض أنه تم حساب $\alpha^k (\text{mod}\, p)$ حيث $k \in \{8,20,16\}$ وكانت نتيجة الحسابات هي:

$$\alpha^8 (\text{mod}\, p) = 10 \Rightarrow 8 \equiv \log_\alpha 2 + \log_\alpha 5 (\text{mod}\, p-1)$$
$$\alpha^{20} (\text{mod}\, p) = 40 \Rightarrow 20 \equiv 3\log_\alpha 2 + \log_\alpha 5 (\text{mod}\, p-1)$$
$$\alpha^{16} (\text{mod}\, p) = 18 \Rightarrow 16 \equiv \log_\alpha 2 + 2\log_\alpha 3 (\text{mod}\, p-1)$$

تحقق من أن نظام التطابقات ليس له حل وحيد $(\log_\alpha 2, \log_\alpha 3, \log_\alpha 5)$.

(ب) أضف التطابق الذي تحصل عليه من $\alpha^1 (\text{mod}\, p) = 2 \cdot 3$ ومن ثم حل النظام (قيمة $\log_\alpha 2$ يجب أن تكون مساوية للقيمة التي حصلنا عليها في المثال (**١١,٥,١**)).

(ج) جد $\log_\alpha 13$ بتطبيق (ب) على $\alpha^k \cdot 13 (\text{mod}\, p)$ حيث $k = 11$.

(**١١,٥,٥**) ليكن p عدداً أولياً و α مولِّداً للزمرة $\mathbb{Z}_p^*$. بين أن المرتبة الثنائية الأقل أهمية للعدد x يمكن حسابها بفعالية من $\alpha^x (\text{mod}\, p)$.

(١١,٥,٦) ناقش باخ (انظر [2]) العلاقة بين تحليل الأعداد وحساب اللوغاريتمات. على وجه الخصوص يبين هذا التمرين أن وجود خوارزمية لحساب x حيث $a^x \equiv b(\bmod n)$ يؤدي إلى خوارزمية احتمالية لتحليل عدد مؤلف n. لنفرض أن $n = pq$ حيث $p \neq q$ عددان أوليان فرديان. ولنفرض أن $\lambda = lcm\left(\varphi(p), \varphi(p)\right)$.

(أ) أثبت أن $K = \left\{z \in \mathbb{Z}_n^* : z^{\lambda/2} \equiv \pm 1(\bmod n)\right\}$ هي زمرة جزئية فعلية من $\mathbb{Z}_n^*$. استنتج أن على الأقل نصف عناصر $\mathbb{Z}_n^*$ لا تنتمي إلى K.

(ب) لنفرض أن $a \in \mathbb{Z}_n^* \setminus K$ وأن $a^x \equiv 1(\bmod n)$ حيث $x \neq 0$ (يسمى قوة a). أثبت وجود $0 < k < \log_2 x$ حيث $a^{x/2^k}$ جذر تربيعي غير تافه للعدد 1 (أي أن $a^{x/2^k} \not\equiv \pm 1$ وأن $\left(a^{x/2^k}\right)^2 \equiv 1$).

(ج) استنتج أن $\left(a^{x/2^k} + 1, n\right)$ قاسم غير تافه للعدد n.

نحصل الآن على خوارزمية التحليل التالية التي تستخدم الخوارزمية $a^x \equiv b(\bmod n)$ لإيجاد قوة للعدد a. على الرغم من أن $\varphi(n)$ غير معلوم، إلا أنه يوجد r من بين أول $\log_2 n$ عدد أولي حيث $(r, \varphi(n)) = 1$. لهذا العدد r تقدم الخوارزمية حلاً y للتطابق $\left(a^r\right)^y \equiv a(\bmod n)$ وقوة $x = ry - 1$ للعدد a.

(١١,٦) حواشي
Notes

معظم المادة التي قدمت في هذا الفصل هي مادة تقليدية يمكن إيجادها في عديد من الكتب الجيدة. على سبيل المثال (انظر [74] و [50]). الفصلان الثاني والثالث من [63] يغطيان بعض المادة المهمة ويحتوي على عديد من المراجع. يقدم [50] عديد من الأمثلة لحساب الزمن اللازم (بدلالة عدد العمليات الثنائية) للعمليات الحسابية وهو موضوع نادراً ما تجده في كتب نظرية الأعداد.

الفصل الثاني عشر

أنظمة التعمية ذوات المفتاح المعلن
Public–Key Cryptography

الخاصية الأساسية التي تميز بين أنظمة التعمية ذوات المفتاح المعلن وأنظمة التعمية التقليدية (أنظمة التعمية ذوات المفتاح المتماثل) هي الفصل بين عمليتي التعمية وكشف المعمى. ولكي نكون أكثر دقة، يتكون المفتاح k في أنظمة التعمية ذوات المفتاح المعلن من زوج مرتب $k=(e,d)$ حيث يستخدم e للتعمية و d لكشف المعمى. وفي هذا الإطار يكون e مفتاح معلن و d مفتاح سري يحتفظ فيه فقط من يحتاج لكشف الرسائل المعماة. ولكي يكون النظام آمناً كنظام تعمية يجب أن يكون من الصعب على العدو الذي بحوزته e والنص المعمى c من حساب m حيث $E_e(m)=c$.

كان أول ظهور لفكرة أنظمة التعمية ذوات المفتاح المعلن في العام ١٩٧٦م أثناء محاولة ديفي (Diffie) وهيلمان (Hellman) توزيع مفاتيح عبر قناة غير آمنة ولكنها موثوقة. إن هذا يعني في إطار الشكل (١٠,١) أن كل من أليس وبوب متأكدين من أصل وموثوقية الاتصالات عبر قناة غير آمنة مع وجود تنصت من قبل العدو حواء. والمسألة هنا هي المحافظة على السرية (على الرغم من تنصت حواء على قناة الاتصال) دون الاعتماد على جزء القناة السري في الشكل لنقل المفاتيح أو أي معلومات أخرى. الخطة المطروحة لتبادل المفاتيح هي على النحو التالي:

يختار كل من أليس وبوب عدداً أولياً p ومولِّداً α للزمرة $\mathbb{Z}_p^*$ ويعلنان عنهما. تختار أليس سراً عددًا عشوائيًا a ، $1 \leq a < p$ ثم ترسل α^a إلى بوب علنا (على مرأى وسماع حواء)(١). وبالمثل، يختار بوب سراً عدداً عشوائيًا b ، $1 \leq b < p$ ويرسل α^b إلى أليس. تقوم أليس بحساب $\left(\alpha^b\right)^a \pmod p$ ويقوم بوب بحساب $\left(\alpha^a\right)^b \pmod p$. وبهذا يحصلان على المفتاح السري المشترك $k = \alpha^{ab} \pmod p$ ويستخدمانه بعد ذلك كمفتاح تعمية لنظام تقليدي مثل نظام DES. من المؤكد أن حواء تتمنى معرفة المفتاح السري k ولكي تستطيع ذلك يكون عليها حل مسألة ديفي وهيلمان (DHP) المرتبطة بمسألة اللوغاريتم المنفصل (DHP).

DHP : إذا كان p عدداً أولياً وكان α مولِّداً للزمرة $\mathbb{Z}_p^*$ وإذا علمت α^a و α^b فجد α^{ab}.

DLP : إذا كان p عدداً أولياً وكان α مولِّداً للزمرة $\mathbb{Z}_p^*$ وإذا علمت α^x فجد x.

من الواضح أن DHP ≤ DLP. أي يمكن حل مسألة DHP بزمن حدودي بمعرفة خوارزمية حدودية لحل مسألة DLP. وفي بعض الحالات الخاصة يكون أيضاً DLP ≤ DHP ولكن الحالة العامة مسألة تنتظر الحل (انظر [63]). يعتمد أمن اتفاقية ديفي وهيلمان لتبادل المفاتيح على افتراض صعوبة حل مسألة DHP.

تستخدم أنظمة التعمية ذوات المفتاح المعلن للتغلب على بعض الصعوبات التي تواجهها أنظمة التعمية التقليدية. فمثلاً، تقترح اتفاقية ديفي وهيلمان لتبادل المفاتيح إمكانية المحافظة على سرية التواصل من خلال قنوات غير آمنة (من المهم هنا افتراض موثوقية قناة الاتصال حيث إن اتفاقية تبادل المفاتيح ليست آمنة بوجود عدو نشط وسنوضح ذلك في البند (**١٢,٥**)) ولذا نستطيع القول إن توزيع المفاتيح لا يحتاج إلى

---

(١) α^a يعني $\alpha^a \pmod p$ ولكننا حذفنا "$\bmod p$" للسهولة طالما أن المعنى واضح من السياق.

ناقل مؤتمن بافتراض إمكانية توثيق المفاتيح المعلنة. وبما أنه من المفترض أن يكون التوثيق أسهل من تبادل المفاتيح السرية لأنظمة التعمية التقليدية فنرى عدم ضرورة شرط السرية في أنظمة التعمية ذوات المفتاح المعلن.

ومن الميزات الأخرى لأنظمة التعمية ذوات المفتاح المعلن هي استخدام عدد أقل من المفاتيح. على سبيل المثال، إذا كان عدد مستخدمي نظام تعمية هو n فنحتاج إلى توزيع $\binom{n}{2}$ من المفاتيح في النظام التقليدي مقارنة مع توزيع $2n$ من المفاتيح في النظام المعلن وهو توفير كبير وخاصة عندما يكون n كبيراً.

أحد التطبيقات الأخرى على أنظمة التعمية ذوات المفتاح المعلن هو التوقيع الإلكتروني (Digital Signature) الذي سنناقشه في البنود اللاحقة. في هذه التطبيق يكون بمقدور أليس توقيع رسالة بطريقة تقنع بها بوب أن الرسالة مصدرها هو بالفعل أليس. وأكثر من ذلك حيث يستطيع بوب أيضاً إقناع مصدر ثالث بذلك. المشكلة الأساسية في استخدام أنظمة التعمية التقليدية في التوقيع الإلكتروني تكمن في أن المعلومات التي بحوزة أليس هي نفس المعلومات التي بحوزة بوب، ولذا فهما بحاجة إلى مصدر ثالث موثوق للتوقيع، وهذه المشكلة محلولة عند استخدام أنظمة التعمية ذوات المفتاح المعلن حيث تزودنا هذه الأنظمة بحل رياضي عملي لهذه المشكلة.

(١٢,١) دوال الاتجاه الواحد ودوال التمويه
One-Way And Hash Functions

نناقش في هذا البند مفهومين أساسين للتعمية، هما دوال الاتجاه الواحد ذوات الباب السري وهذا المفهوم من أساسيات أنظمة التعمية ذوات المفتاح المعلن. أما المفهوم الآخر والشائع الاستخدام في خطط التوقيع الإلكتروني فهو دوال التمويه (أو الدوال التعموية).

دوال الاتجاه الواحد

نقول إن الدالة $f : M \to C$ دالة اتجاه واحد إذا كان من السهل حساب $f(m)$ لكل $m \in M$ ولكن لكل $c \in C$ من الصعب حسابياً إيجاد m يحقق $f(m) = c$. يعتقد أن الدالة التي قدمناها في البند (**١٠,٣,٢**) لكلمات السر المستخدمة في يونكس (Unix) هي دالة اتجاه واحد (تحت سقف بعض القدرات الحسابية) حيث يتم تخزين (كلمة السر واسم المستخدم) f عوضاً عن كلمة السر نفسها[٢]. ودالة أخرى يعتقد أنها دالة اتجاه واحد هي دالة القوة المنفصلة. أي الدالة $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^*$ المعرفة بالقاعدة $f(a) \equiv \alpha^a \pmod p$ حيث p عدد أولي و α مولِّداً للزمرة $\mathbb{Z}_p^*$.

لا يوجد برهان رياضي على وجود دوال اتجاه واحد. ولذا فأنظمة التعمية ذوات المفتاح المعلن تفترض أن بعض الدوال المعينة هي دوال اتجاه واحد آمنة للفترة المستخدمة. سنناقش في البنود القادمة بعض دوال الاتجاه الواحد المستخدمة في أنظمة التعمية ذوات المفتاح المعلن.

نقول إن دالة اتجاه واحد هي دالة ذات باب سري (trapdoor) إذا توفرت معلومات اضافية تسمح بإيجاد m يحقق $f(m) = c$ لكل c. دوال الاتجاه الواحد ذوات الباب السري هي الدوال المستخدمة في أنظمة التعمية ذوات المفاتيح المعلنة.

مثال (١٢,١,١) (تطبيقات على دوال الباب السري)

المحافظة على السر (Confidentiality): يختار كل مستخدم A دالة اتجاه واحد ذات باب سري خاصة به f_A ثم يعلن عنها. لإرسال رسالة سرية m إلى A يقوم المرسل باستخدام f_A ومن ثم يرسل الرسالة $c = f_A(m)$. وبما أن A هو الوحيد الذي لديه

---

(٢) كان هناك اعتقاد أن القيم المخزنة معلومة لجميع مستخدمي النظام مما يؤدي إلى كسر النظام ومن ثم معرفة كلمة السر حيث أن معظم المستخدمين للنظام يستعلمون كلمات سر سهلة التخمين. تطلب الأنظمة الحديثة كلمات سر أفضل وتقوم بتخزين المعلومات بشكل سري.

المعلومات السرية التي تسمح بإيجاد معكوس f_A فيكون بإمكانه معرفة الرسالة $m = f_A^{-1}(c)$. لاحظ عدم استطاعة المرسل من الحصول على m من c. لم نحتاج في هذه التطبيق إلى تبادل المرسل و المستقبل معلومات سرية ولكن من الضروري التأكد من موثوقية المفتاح المعلن.

منع التزوير (non-repudiation): هذا التطبيق هو رديف التوقيع الكتابي. المطلوب هو توقيع أليس لرسالة m بحيث يكون بإمكان بوب اقناع طرف ثالث بأن مصدر الرسالة m هو بالفعل أليس. لنفرض أن m مذيلة بمعلومات زائدة. إذا كانت $f_A : M \to M$ هي دالة اتجاه واحد ذات باب سري التي اختارتها أليس فإنها تقوم بإرسال $s = f_A^{-1}(m)$ إلى بوب. يقوم بوب بحساب $m = f_A(s)$ وتكون الرسالة الموقعة هي الزوج المرتب (m, s). من الممكن أن يكون باستطاعة العدو حساب $m = f_A(s)$ لنص مختار s ولكن تذيل m يمنع مثل هذا التزوير. وإذا كانت السرية مطلوبة في هذا التواصل فبإمكان أليس إرسال $c = f_B(s)$ عوضاً عن s حيث f_B دالة الاتجاه الواحد ذات الباب السري التي اختارها بوب.

دوال التمويه التعموية

نقول إن $H : X \to Y$ دالة تمويه إذا لم تكن دالة أحادية. لكل $x \in X$ يسمى $H(x)$ تمويه x ويستخدم كمعَرِّف للعنصر x. وبما أن H دالة غير أحادية فلابد من وجود $x_1 \neq x_2$ بحيث يكون $H(x_1) = H(x_2)$. من بين أهداف إنشاء دالة تمويه هي وضع شروط تفصل بين التصادمات ووجود خوارزمية فعالة لحساب قيم التمويه $H(x)$.

في العادة تكون عمليات التعمية في أنظمة التعمية ذوات المفتاح المعلن مكلفة حسابياً وعملية توقيع رسائل طويلة يحتاج زمن طويل. ولهذا أثناء التطبيق العملي تستخدم دوال التمويه لإنشاء ما يسمى الرسالة الملخصة (message digest) للرسالة المطلوب توقيعها ومن ثم يتم توقيع الرسالة الملخصة. ولكي نضمن أمن هذه العملية فيجب أن تتحقق في دالة التمويه خواص إضافية.

تعريف (١٢,١,٢)

دالة التمويه التعموية هي دالة $H : \{0,1\}^* \to \{0,1\}^*$ تحقق ما يلي :

(١) توجد خوارزمية فعالة لحساب H .

(٢) (مقاومة الصورة العكسية). لكل $y \in \{0,1\}^n$ يكون من الصعب حسابياً إيجاد $x \in \{0,1\}^*$ حيث أن $H(x) = y$.

(٣) (مقاومة التصادم). يكون من الصعب حسابياً إيجاد $x_1 \neq x_2 \in \{0,1\}^*$ حيث $H(x_1) = H(x_2)$.

حتى الآن لم يتم البرهان على وجود دوال تمويه تعموية ؛ (لأن الشرطين (١) و (٢) يؤديان إلى أنها دالة اتجاه واحد)، ومع ذلك يستخدم عدد من الدوال التي يعتقد أنها دوال تمويه تعموية في التحقق من صواب البيانات وخطط التوقيع.

مثال (١٢,١,٣) (تطبيق على التوقيعات)

لتوقيع رسالة m ، تقوم أليس بحساب التمويه وتوقيعه وبعد ذلك ترسل كل من الرسالة والتوقيع على $H(m)$ إلى بوب الذي يقوم بحساب $H(m)$ والتحقق من صواب التوقيع. تسمى الخطة الذي تتطلب وجود الرسالة نفسها أثناء عملية التحقق بالتوقيع الإلكتروني مع الملحق (digital signature scheme with appendix). ▲

إذا لم تكن دالة التمويه H مقاومة للصورة العكسية فبإمكان العدو (وربما بوب) بعد أن يحصل على توقيع صائب على $H(m)$ من تزوير توقيع أليس وذلك بإيجاد رسالة m' *تحقق* $H(m') = H(m)$ ومن ثم الحصول على توقيع صائب للرسالة m' .

إذا كان $m \neq m'$ حيث $H(m) = H(m')$ فباستطاعة أليس الخداع بحيث توقع الرسالة m وتدعي أن الرسالة التي وقعتها هي m' . ومن الممكن أن يجد العدو مثل هذا التصادم ومن ثم يقنع أليس بالتوقيع على إحدى الرسالتين.

افترضنا في المثال السابق أن التوقيع يضمن عدم التلاعب في التمويه الذي قامت أليس بحسابه. وبصورة عامة إذا وجدت آلية لحماية قيمة التمويه فيكون باستطاعتنا

استخدام دالة التموية للتحقق من عدم التلاعب في البيانات المقابلة لذلك. وفي هذا الإطار، تسمى دالة التمويه هذه التي لا تحتاج إلى مفتاح سري (مفتوحة)، شفرة اكتشاف معدلة (modification detection code) أو اختصاراً MDC. أما دالة التمويه التي تحتاج إلى مفتاح سري (مقفولة) لتوثيق مصدر البيانات فتدعى شفرة توثيق رسالة (message authentication code)، اختصاراً MAC. الدالة CBC-MAC المقدمة في البند (**١٠,٣,٢**) مثال على مثل هذه الدوال.

يوجد عديد من دوال التمويه التي يتم تصميمها باستخدام أنظمة التعمية القالبية، أحدها هي الدالة المقفولة CBC-MAC ودالتين مفتوحتين نقدمهما في المثالين التاليين.

مثال (١٢,١,٤) (تمويه ماتياس وماير وأوسيز)

لنفرض أن E نظام تعمية قالبي حيث $\mathcal{K}$ فضاء المفاتيح. لنفرض أن $E_k : \{0,1\}^n \to \{0,1\}^n$ وأن $g : \{0,1\}^n \to \mathcal{K}$ دالة معلنة وأن H_0 قيمة ابتدائية معلنة تنتمي إلى $\{0,1\}^n$. تعرف الدالة $H : \{0,1\}^* \to \{0,1\}^n$ على النحو التالي:

(١) نفرض أن $x = x_1x_2 \ldots x_t$ حيث x_i كلمة ثنائية طولها n.

(٢) نفرض أن $H_i = E_{g(H_{i-1})}(x_i) \oplus x_i$ ، $1 \leq i \leq t$. عندئذ، $H(x) = H_t$.

يبين الشكل (**١٢,١**أ) مخطط هذه الدالة. ▲

إذا بدلنا x_i مع H_{i-1} في المثال السابق فسنحصل على دالة التمويه التالية مع ملاحظة التغيير في كتابة x.

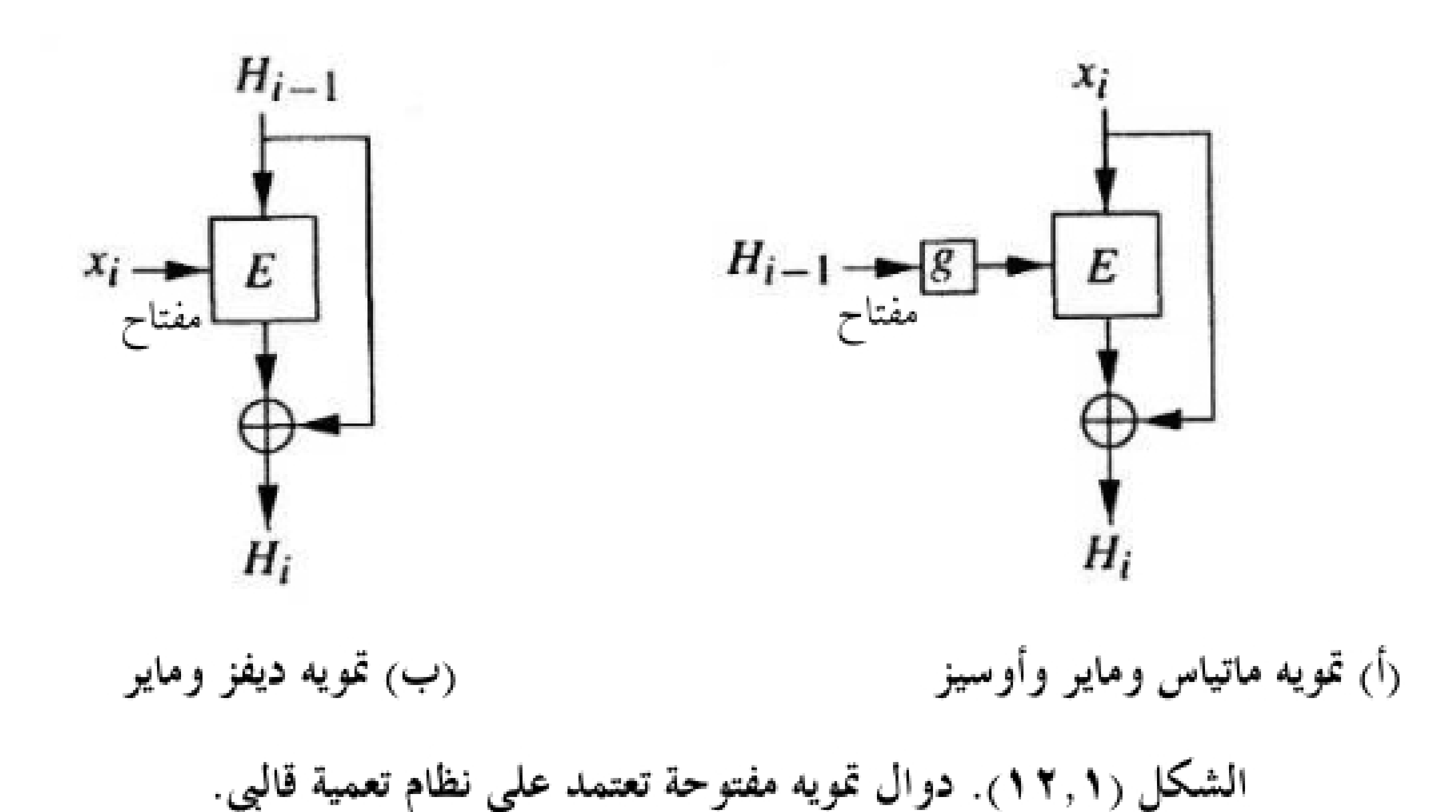
مثال (١٢,١,٥) (تمويه ديفز وماير)

لنفرض أن E نظام تعمية قالبي طول قالبه يساوي n مرتبة ثنائية ويستخدم مفاتيح طول كل منها يساوي k مرتبة ثنائية. لنفرض أن H_0 قيمة ابتدائية معلنة تنتمي إلى $\{0,1\}^n$. تعرف الدالة $H : \{0,1\}^* \to \{0,1\}^n$ على النحو التالي:

(١) نفرض أن $x = x_1x_2 \ldots x_t$ حيث x_i كلمة ثنائية طولها k.

(٢) نفـــرض أن $H_i = E_{x_i}(H_{i-1}) \oplus H_{i-1}$ حيـــث $1 \leq i \leq t$. عندئـــذ، $H(x) = H_t$.

مخطط هذه الدالة مبين في الشكل (**١٢,١ب**).



(أ) تمويه ماتياس وماير وأوسيز **(ب) تمويه ديفز وماير**

الشكل (١٢,١). دوال تمويه مفتوحة تعتمد على نظام تعمية قالبي.

يجب أن يكون طول الرسالة المدمجة التي تولدها دالة تمويه مفتوحة كافياً لمنع هجوم تاريخ الميلاد (بحث عشوائي للحصول على تصادم). من المتوقع الحصول على تصادم في دوال التمويه ذات الطول n بعد $2^{n/2}$ عملية على الأكثر. على وجه الخصوص كل من دالتي التمويه المقدمتين في الشكل (**١٢,١**) غير محصنة لمنع التصادم إذا كان $E = DES$. طول الرسالة المدمجة لدالة التمويه المشهورة المعروفة باسم خوارزمية التمويه الآمنة (secure hash algorithm) أو اختصاراً $SHA - 1$ يساوي 160 مرتبة ثنائية وطول الرسالة المدمجة لدالة تمويه مشهورة أخرى تدعى الرسالة المدمجة الخامسة أو اختصاراً $MD5$ يساوي 128 مرتبة ثنائية (كلا الدالتين يعتمد على $MD4$ والرمز MD يعني خوارزمية رسالة ملخصة والرقم 4 يعني ترتيب الخوارزمية في سلسلة خوارزميات قدمها رايفست).

تمارين

(١٢,١,٦) لنفرض أن $g : \{0,1\}^* \to \{0,1\}^*$ دالة تمويه مقاومة للتصادم. ولنفرض أن الدالة h معرفة على النحو التالي:

$$h(x) = \begin{cases} 1 \,||\, x & , \quad \text{إذا كان طول } x \text{ يساوي } n \text{ مرتبة ثنائية} \\ 0 \,||\, g(x) & , \quad \text{ما عدا ذلك} \end{cases}$$

حيث الرمز ' || ' يعني ضم أو تسلسل (concatenation). أثبت أن h دالة تمويه طولها $n + 1$ مقاومة للتصادم ولكنها ليست مقاومة للصورة العكسية (انظر [63] ، ملحوظة (**٩,٢٠**)).

(١٢,١,٧) هذا التمرين هو المثال (**٩,٦٤**) من [63] ويبين الحيطة الواجب أخذها عند إنشاء MAC من MDC. لنفرض أن h هي MDC معرفة استقرائياً على رسالة $x = x_1 \ldots x_t$ على النحو التالي:

$$H_i = f(H_{i-1}, x_i)$$
$$h(x) = H_t$$

حيث H_0 هي قيمة ابتدائية معطاة. يمكن تحويل h إلى MAC بضم مفتاح سري k بحيث تكون MAC على الرسالة x هي:

$$M = h(kx)$$

أثبت إمكانية استخدام معرفة الزوج المرتب (M, x) في تزوير MAC على xy دون الحاجة لمعرفة المفتاح السري k.

(١٢,١,٨) هذا التمرين مأخوذ من التمرين (**٧,٤**) (انظر [86]). لنفرض أن p و q عددان أوليان حيث كل من $p' = 2p + 1$ و $q' = 2q + 1$ عدداً أولياً. ولنفرض أن $n = p'q'$. لنفرض أيضاً أن $\alpha \in \mathbb{Z}_n^*$ من الرتبة $2pq$. لتكن الدالة $h : \mathbb{Z} \to \mathbb{Z}_n^*$ معرفة بالقاعدة:

$$h(x) \equiv \alpha^x (\operatorname{mod} n)$$

إذا كان $h(x_1) = h(x_2) = h(x_3)$ فأثبت وجود خوارزمية فعالة لتحليل n بمعرفة تصادم مناسب على x_i. وضح الخوارزمية عندما يكون $n = 77$ و $\alpha = 2$ حيث $h(9) = h(69) = h(129)$.

(١٢,٢) نظام RSA
RSA Cipher

يستخدم نظام RSA المشهور الذي تم اكتشافه في العام ١٩٧٧م من قبل رايفست وشامير وأدلمان (Rivest, Shamir, and Adleman) في أغراض التعمية وخطط التوقيع الإلكتروني. يعتمد أمن نظام RSA على فرضية صعوبة مسألة تحليل الأعداد. يعرف نظام RSA على النحو التالي:

(١) لنفرض أن $p \neq q$ عددان أوليان كبيران وأن $n = pq$ و $\varphi = (p-1)(q-1)$.

(٢) اختار قوة تعمية عشوائياً e، $1 < e < \varphi$ حيث $(e, \varphi) = 1$.

(٣) استخدم خوارزمية إقليدس لإيجاد قوة كشف المعمى d، $1 < d < \varphi$ حيث $ed \equiv 1 (\bmod \varphi)$.

(٤) عرف $f : \mathbb{Z}_n \to \mathbb{Z}_n$ على النحو التالي:

$$f(m) \equiv m^e (\bmod n)$$

يعتقد أن دالة RSA (الدالة f) هي دالة اتجاه واحد ذات باب سري d. فإذا كان d معلوماً فتوجد خوارزمية فعالة لإيجاد m من $c = f(m)$ وذلك باستخدام الخاصية $ed \equiv 1 (\bmod \varphi)$. لإثبات ذلك، نفرض أولاً أن $p \nmid m$. بما أن:

$$ed = 1 + k\varphi = 1 + k(p-1)(q-1)$$

حيث $k \in \mathbb{Z}$ وأن $m^{p-1} \equiv 1 (\bmod p)$ (استناداً إلى مبرهنة فيرما الصغرى) نجد أن:

$$m^{ed} = m^{1+k\varphi} = m\left(m^{p-1}\right)^{k(q-1)} \equiv m (\bmod p)$$

أما إذا كان $p \mid m$ فنجد أن $m^{ed} \equiv 0 \equiv m(\bmod p)$. وبالمثل، يمكن إثبات أن:

$$m^{ed} \equiv m(\bmod q)$$

وبما أن p و q أوليان نسبياً فنخلص إلى أن:

$$m^{ed} \equiv m(\bmod n)$$

إذن،

$$c^d \equiv \left(m^e\right)^d \equiv m(\bmod n)$$

وبهذا يمكن إيجاد m من c باستخدام خوارزمية التربيع وهي خوارزمية فعالة.

تسمى مسألة إيجاد f^{-1} دون معرفة d مسألة RSA وتنص على:

لنفرض أن $n = pq$ حيث $p \neq q$ عددان أوليان ولنفرض أن e عدد صحيح موجب أولي نسبياً مع $\varphi = (p-1)(q-1)$ وأن c عدد صحيح. جد m بحيث يكون: $m^e \equiv c(\bmod n)$.

إذا كان تحليل n معلوماً فمن الممكن حساب d ومن ثم الحصول على m بطريقة فعالة. ولكن من المعلوم أن تحليل n حيث p و q عددان أوليان مختاران بعناية مسألة صعبة المنال.

يقدم التمرين (**١٢,٢,١٢**) خوارزمية فعالة لتحليل n إذا علمنا قيمة d. وبهذا تكون مسألة تحليل n ومسألة حساب d بمعرفة n و e متكافئتان حسابياً. بهذا التكافؤ يكون لدينا دليل على أن مسألة RSA ومسألة تحليل n هما مسألتان درجة صعوبتهما متساوية ولكن لم يتم تقديم برهان رياضي لذلك[٣].

في نظام RSA، المفتاح المعلن هو (n,e) والمفتاح السري هو d. إذا كان $0 \leq m \leq n-1$ فإن تعمية m هي:

$$c \equiv m^e(\bmod n)$$

(٣) قدم كل من بونيه وفانكاتيسان (Boneh and Venkatesan) في المرجع [15] دليلاً على أن كسر نظام RSA حيث قوة التعمية e صغيرة لا يمكن أن تكافئ مسألة التحليل.

وكشف المعمى هو :

$$. m = c^d (\bmod n)$$

مثال (١٢,٢,١) (مثال صفي على RSA)

لنفرض أن العددين $p = 7$ و $q = 13$ استخدما لتوليد مفتاح نظام RSA. عندئذ :

$$\varphi = (p-1)(q-1) = 72$$

ولنفرض أن $e = 5$. باستخدام الشرط :

$$ed \equiv 1 (\bmod \varphi)$$

نجد أن قوة كشف المعمى هو $d = 29$. المفتاح المعلن هو $(n = 91, e = 5)$ والمفتاح السري هو $d = 29$. الرسائل m هي أعداد صحيحة تقع في الفترة $[0, 91)$.
إذا كان $m = 23$ فنجد أن :

$$c \equiv m^e \equiv 23^5 \equiv 4 (\bmod 91)$$
$$c^d \equiv 4^{29} \equiv 23 (\bmod 91)$$

حيث استخدمنا خوارزمية التربيع في الحسابات. ▲

عند استخدام نظام RSA لتعمية رسائل فمن الممكن أن تكون تعمية بعض الرسائل هي ذاتها، أي توجد m بحيث يكون $c \equiv m^e \equiv m (\bmod n)$. على سبيل المثال، تعمية كل من الرسائل $m \in \{0, 1, n-1\}$ هي ذاتها (لاحظ أن قوة التعمية e عدد فردي). لإيجاد جميع هذه الرسائل، لاحظ أولاً أن $m^e \equiv m (\bmod n)$ إذا وفقط إذا كان $m^e \equiv m (\bmod p)$ و $m^e \equiv m (\bmod q)$.

الآن، إذا كـــان $m^e \equiv m (\bmod p)$ فإمـــا أن $m \equiv 0 (\bmod p)$ أو أن $m^{p-1} \equiv 1 (\bmod p)$. ومن ثم استناداً إلى التمرين (**١١,١,٢٢**) نجد أن عدد الحلول هو $1 + (e-1, p-1)$. وبالمثل، عدد حلول التطابق $m^e \equiv m (\bmod q)$ يساوي $1 + (e-1, q-1)$. وباستخدام مبرهنة الباقي الصينية نجد أن عدد حلول التطابق $m^e \equiv m (\bmod n)$ يساوي $[1 + (e-1, p-1)][1 + (e-1)(q-1)]$. على وجه

الخصوص، بما أن كلاً من e و p و q فردي فيوجد على الأقل 9 رسائل تعمى إلى ذاتها. في المثال (١٢,٢,١) يوجد 15 رسالة تعمى إلى ذاتها، احدى هذه الرسائل هي $m = 8$. التمرين (١٢,٢,٣) يبين عملية تعمية جميع رسائلها تعمى إلى ذاتها.

في العادة لا تستخدم طريقتي معرفة أو اختيار النص الواضح لكسر أنظمة التعمية ذوات المفاتيح المعلنة. ولكن من الممكن كسر النظام بطريقة اختيار النص المعمى ويتم ذلك على النحو التالي: لنفرض أن حواء (العدو) اختارت رسالتين معميتين c_1 و c_2 وحسبت النصين الواضحين m_1 و m_2 على التوالي في نظام RSA. عندئذ،

$$(m_1 m_2)^e \equiv m_1^e m_2^e \equiv c_1 c_2 (\bmod n)$$

ومن ذلك نرى أن $c \equiv c_1 c_2 (\bmod n)$ هي تعمية الرسالة $m \equiv m_1 m_2 (\bmod n)$. الآن، تقوم حواء باختيار $x \in \mathbb{Z}_n^*$ وترسل $\bar{c} = cx^e$ إلى أليس لغرض كشف المعمى. عندئذ، تحصل أليس على النص الواضح $\bar{m} \equiv \left(\bar{c}\right)^d (\bmod n)$. وبما أن:

$$\bar{m} = (\bar{c})^d \equiv \left(cx^e\right)^d \equiv c^d x^{ed} \equiv mx (\bmod n)$$

فيكون بإمكان حواء الحصول على الرسالة m وهي:

$$m \equiv \bar{m} x^{-1} (\bmod n)$$

يمكن لواضع التعمية هزيمة مثل هذا الهجوم بإضافة بعض المعلومات الزائدة على الرسائل الواضحة قبل تعميتها.

من المهم أن يكون عدد القياس في مفتاح نظام RSA كبيراً جداً لضمان عدم القدرة على تحليله. اقترح مينيزس (Menezes) في العام ١٩٩٦م أن يكون طول n أكبر من أو يساوي 768 مرتبة ثنائية ورشح أن يكون هذا الطول يساوي 1024 مرتبة ثنائية لضمان أمن طويل الأجل (انظر [63]). أما في العام ١٩٩٩م استنتج كل من لينسترا وفيرهول (Lenstra and Verheul) أن 768 مرتبة ثنائية ليست كافية لأمن RSA مقارنة

مع أمن نظام DES (انظر [55]). هناك أيضاً شروطاً إضافية على العددين الأوليين p و q وذلك لتحاشي طرق التحليل المعروفة، على سبيل المثال، يجب أن يكون p و q من الطول نفسه ولا يجب أن يكون $|p-q|$ صغيراً نسبياً.

خطة توقيع نظام RSA (مع معرفة الرسالة)

يمكن استخدام نظام RSA لتوقيع الرسائل إلكترونياً على النحو التالي:

إذا أرادت أليس توقيع الرسالة m فيكون التوقيع هو $s \equiv m^d (\bmod n)$ حيث d مفتاح أليس السري وترسل s إلى بوب. يقوم بوب بحساب $m \equiv s^e (\bmod n)$ باستخدام مفتاح أليس المعلن (n, e). وبهذا يحصل على الرسالة الموقعة (m, s).

لغرض كشف الرسائل المزورة، لا بد من أن تزود الرسالة ببعض المعلومات الإضافية m قبل توقيعها. فمثلاً، إذا اختار المزور (العدو) s وقام بإرسال $m \equiv s^e (\bmod n)$ إلى بوب مستخدماً مفتاح أليس المعلن. عندئذ، يقبل بوب الرسالة الموقعة (m, s) فقط إذا كانت تتضمن المعلومات الزائدة (حواء ليس لديها هذه المعلومات الزائدة).

عادة يتم اختيار قوة تعمية صغيرة لتسريع عملية التعمية والتحقق من صواب التوقيع، ولكن توجد بعض التحفظات المبينة في التمرينين (**١٢,٢,٤**) و (**١٢,٢,٥**) على مثل هذا الاختيار. وبالمثل، اختيار عدد صغير لقوة كشف المعمى d يمكن أن يحسن من عملية كشف المعمى وزمن توليد التوقيع ولكن بين واينر (Wiener [95]) من إمكانية معرفة المفتاح السري إذا كان d صغيراً مقارنة مع n وذلك باستخدام طريقة الكسور المتواصلة وهذا هو فحوى التمرين (**١٢,٢,٧**).

يستخدم عند التطبيق العملي لنظام RSA نظاماً أكثر تطوراً من النظام الموصوف في هذا البند. تذيل الرسالة قبل تعميتها هو إجراء شائع، وذلك للتغلب على محاولة كسر النظام باختيار النص المعمى وبعض محاولات الكسر الأخرى حيث تذيل الرسالة

بمعلومات عشوائية مع تكرار تعمية الرسالة نفسها يؤدي على الأغلب إلى أربعة رسائل معماة مختلفة (انظر [4]). أجرى بونيه (انظر [12]) مسحاً على محاولات كسر النظام لعقدين من الزمن وكانت النتيجة غير مقلقة حيث أظهرت معظمها أن الخطر يكمن في سوء استخدام نظام RSA. وأخيراً، نلفت نظر القارئ إلى أن التنفيذ الآمن لنظام RSA ليس بالمهمة السهلة.

تمارين

(**١٢,٢,٢**) اختارت أليس $p = 31$ و $q = 47$ و $e = 77$ لاستخدامها في نظام RSA.

(أ) ما هو مفتاح أليس السري؟

(ب) جد النص المعمى للرسالة $m = 3$ باستخدام مفتاح أليس المعلن.

(ج) تحقق من صواب نتيجة الفقرة (ب)، وذلك بالكشف عن الرسالة المعماة لتحصل على الرسالة الأصلية m.

(**١٢,٢,٣**) إذا كان $p = 5$ ، $q = 17$ ، $e = 33$ في نظام RSA فأثبت أن جميع الرسائل تعمى لذاتها.

(**١٢,٢,٤**) يفضل استخدام قوة تعمية صغيرة في نظام RSA لغرض تسريع عملية التعمية. لنفرض أن قوة التعمية لثلاث مستخدمين هي $e = 3$ وأن قياسات نظام RSA هي n_1 ، n_2 ، n_3 على التوالي. اعترضت حواء (العدو) النصوص المعماة:

$$c_i \equiv m^e (\mathrm{mod}\, n_i) \qquad \text{حيث} \qquad 1 \le i \le 3$$

للرسالة الواضحة المشتركة m. إذا افترضنا أن n_i أولية نسبياً مثنى مثنى فبين كيفية استخدام خوارزمية جاوس لمعرفة الرسالة m.

يوضح التمرين السابق بعض نقاط ضعف نظام RSA. في العادة تستخدم قوة تعمية أكبر (مثل $e = 2^{16} + 1$ الذي يحتوي على عدد قليل من المرتبة 1 في التمثيل

الثنائي لضمان الفعالية) للتغلب على الضعف السابق. كما أن توليد كلمة ثنائية عشوائياً وتذيل الرسالة بها قبل إجراء كل عملية تعمية هو أسلوب متبع للتغلب على الضعف الناتج عن استخدام قوة تعمية صغيرة (يدعى هذا الإجراء تمليح (Salting)).

(**١٢,٢,٥**) وصف كوبرسميث (Coppersmith [24]) طريقة فعالة للتغلب على محاولة كسر نظام RSA الذي يستخدم قوة تعمية صغيرة وذلك في حالة تحقيق الرسائل الواضحة لعلاقة خطية معلومة. لنفرض أن قوة التعمية هي $e = 3$ وأن c_1 و c_2 رسالتين معميتان تقابلان الرسالتين الواضحتين m و $m+1$ (حيث m مجهول). أي أن:

$$c_1 \equiv m^3 (\operatorname{mod} n)$$
$$c_2 \equiv (m+1)^3 (\operatorname{mod} n)$$

(أ) أثبت أن:

$$\frac{c_2 + 2c_1 - 1}{c_2 - c_1 + 2} \equiv m (\operatorname{mod} n)$$

أي أنه يمكن معرفة m من النصين المعميين c_1 و c_2.

(ب) لاحظ أن $x - m$ قاسم مشترك للعددين $x^3 - c_1$ و $(x+1)^3 - c_2$. أثبت الصيغة المقدمة في الفقرة (أ) باستخدام خوارزمية إقليدس لإيجاد القاسم المشترك الأكبر للعددين $x^3 - c_1$ و $(x+1)^3 - c_2$. تحقق من أن مخرج الخوارزمية هو بالفعل كثيرة حدود خطية.

(**١٢,٢,٦**) (معرفة جزئية للمفتاح) لنفرض أن $n = pq$ حيث p و q عددان أوليان يحققان $5 \leq p < q < 2p$. ولنفرض أن e و d عددان صحيحان يحققان $1 < e , d < \varphi$ و $ed \equiv 1 (\operatorname{mod} \varphi(n))$.

(أ) بما أن $ed \equiv 1 (\operatorname{mod} \varphi(n))$ فيوجد عدد صحيح k يحقق $ed - k\varphi(n) = 1$. أثبت أن $1 \leq k < e$.

(ب) افرض أن $d_1 = \left\lfloor \frac{kn+1}{e} \right\rfloor$. أثبت أن $\left| d_1 - d \right| < 3\sqrt{n}$.

(ج) إذا كان $e = 3$ فأثبت أن $k = 2$.

(د) إذا علمت فقط القيمتان $e = 3$ و n فصمم خوارزمية فعالة لحساب النصف الأيسر من مراتب d الثنائية (بالتحديد، يفترض أن تختزل الخوارزمية القيم إلى قيمة واحدة أو قيمتين). هذا التمرين مأخوذ من [12].

(١٢,٢,٧) (قوة كشف معمى صغيرة) افرض أن $n = pq$ حيث p و q عددان أوليان يحققان $p < q < 2p$. افرض أن e و d عددان صحيحان يحققان $1 < e , d < \varphi(n)$ و $ed \equiv 1(\bmod \varphi(n))$.

افرض أيضاً أن $d < \frac{1}{3} n^{1/4}$ وأن k عدد صحيح يحقق $ed - k\varphi(n) = 1$.

(أ) أثبت أن $n - \varphi(n) < 3\sqrt{n}$. أي أن n هو تقريب جيد لقيمة $\varphi(n)$.

(ب) أثبت أن $\frac{e}{n}$ هو تقريب جيد للعدد $\frac{k}{d}$. بالتحديد، أثبت أن $\left| \frac{e}{n} - \frac{k}{d} \right| < \frac{1}{2d^2}$.

(ج) استخدم الحقيقة أدناه لتصميم خوارزمية فعالة لحساب d إذا علمت فقط القيمتين n و e .

حقيقة: لنفرض أن $1 \leq x_0 < y_0$ حيث x_0 و y_0 عددان صحيحان. عدد الأزواج المرتبة (x, y) حيث $1 \leq y < y_0$ التي تحقق $\left| \frac{x_0}{y_0} - \frac{x}{y} \right| < \frac{1}{2y^2}$ محدوداً بالمقدار $2 \log_2 y_0$. إضافة إلى ذلك من الممكن إيجاد جميع هذه الأزواج المرتبة بخوارزمية فعالة (كمتقاربات للكسور المتواصلة للعدد $\frac{x_0}{y_0}$. انظر هاردي ورايت (Hardy and Wright [95]). هذه الطريقة لكسر النظام أخذت من [12,14] وتم اكتشافها من قبل واينر [95].

(**١٢,٢,٨**) (هجوم التحليل الخاطئ [13,47]) لنفرض أن بطاقة ذكية (smartcard) تستخدم مبرهنة الباقي الصينية لكشف المعمى في نظام RSA. أي أن كشف النص المعمى c يتم بحساب:

$$m_p \equiv c^{d \bmod (p-1)} \pmod p$$
$$m_q \equiv c^{d \bmod (q-1)} \pmod q$$

وبعد ذلك نجد m ، $0 \le m < n$ الذي يحقق:

$$m \equiv m_p \pmod p$$
$$m \equiv m_q \pmod q$$

(أ) أثبت أن العملية تؤدي إلى كشف معمى صحيح. أي، أثبت أن $m \equiv c^d \pmod n$.

(ب) لنفرض إمكانية التعديل في البطاقة الذكية بحيث تحسب قيمة خاطئة m_p وتحسب قيمة صائبة m_q. لنفرض أن m' هو كشف المعمى الخاطئ للرسالة c الذي نحصل عليه بعد التعديل. أثبت إمكانية استخدام ذلك لتحليل n.

(**١٢,٢,٩**) هجوم دوري لكسر نظام RSA بإيجاد أصغر عددٍ صحيحٍ موجبٍ k يحقق $c^{e^k} \equiv c \pmod n$.

(أ) أثبت أن هذا العدد k موجود. ثم أثبت أن حواء (العدو) تستطيع الحصول على الرسالة الواضحة من $c^{e^{k-1}} \equiv m \pmod n$.

(ب) يمكن تعميم هذا الهجوم على النحو التالي:

نفرض أن u هو أصغر عدد صحيح موجب يحقق $1 < \left(c^{e^u} - c, n\right)$. أثبت أن العدو يستطيع الحصول على قاسم غير تافه للعدد n أو أن ذلك يؤدي إلى الحصول على الهجوم الدوري الأساسي (أي أن $u = k$).

في الغالب الهجوم الدوري هذا لا ينجح بكسر النظام إذا كان $n = pq$ حيث قواسم $p - 1$ و $q - 1$ أعداد كبيرة جداً (انظر [63]). أما الهجوم الدوري المعمم فمن المتوقع توقفه قبل الدورة الأساسية ومن ثم يمكن النظر إليه على أنه كسر للنظام بمحاولة تحليل العدد. وبهذا فإن حظوظ نجاحه محدودة على اعتبار أن مسألة التحليل صعبة.

(**١٢,٢,١٠**) أثبت إمكانية استخدام القوة الشاملة (universal exponent) $\lambda(pq) = lcm(p-1, q-1)$ عوضاً عن $\varphi(n)$ لتوليد مفتاح نظام RSA. من الممكن أن يؤدي استخدام λ إلى قوة كشف معمى صغيرة.

(**١٢,٢,١١**) الحاجة إلى أعداد أولية كبيرة لتوليد مفتاح RSA. لنفرض أن مخرج اختبار أوليات احتمالي هو "محتمل أولي" حيث p هو في الحقيقة عدد مؤلف. لنفرض أن $p = p_1 p_2$ حيث $p_1 \neq p_2$ عددان أوليان مختلفان عن q. أثناء توليد المفتاح نحصل على e و d من $\varphi(p,q) = (p-1)(q-1)$ عوضاً عن الحصول عليهما من $\varphi(n) = (p_1 - 1)(p_2 - 1)(q - 1)$.

(أ) لاحظ أن $\lambda = lcm(p_1 - 1, p_2 - 2, q - 1) \mid \varphi(n)$.

إذا كان $\lambda \mid \varphi(p,q)$ فأثبت أن ذلك يؤدي إلى تعمية وكشف معمى صائبان.

(ب) استخدم $p = 15$ ، $q = 5$ لتوضيح الفقرة (أ). أي، احسب λ ، $\varphi(n)$ ، $\varphi(p,q)$.

(ج) افرض أن $p = 21$ و $q = 5$. أثبت أن λ لا يقسم $\varphi(p,q)$. جد d إذا كان $e = 3$. جد رسالة m بحيث يكون $c^d \not\equiv m (\bmod n)$ ولكن $c \equiv m^e (\bmod n)$.

(**١٢,٢,١٢**) الغرض من هذا التمرين هو إثبات أن معرفة قوة كشف المعمى في d نظام RSA تؤدي إلى وجود خوارزمية فعالة لتحليل n. الفكرة الأساسية هي الحصول على جذر تربيعي غير تافه للعدد 1 قياس n.

بما أن $ed \equiv 1 (\bmod \varphi)$ فإن $m^{ed-1} \equiv 1 (\bmod n)$ لكل $m \in \mathbb{Z}_n^*$. ضع $ed - 1 = 2^s t$ حيث t عدد فردي. يتألف البرهان بإثبات أنه يوجد $r \in [1, s]$ لعلى الأقل نصف الأعداد بحيث يكون:

$$m^{2^{r-1}t} \not\equiv \pm 1 (\bmod n)$$
$$m^{2^r t} \equiv 1 (\bmod n)$$

ومن ثم لمثل هذا العدد m يكون $(m^{2^{r-1}t} - 1, n)$ قاسماً غير تافه للعدد n.

يفشل $m \in \mathbb{Z}_n^*$ بالحصول على قاسم عندما يكون $m^t \equiv 1 (\bmod n)$ أو إذا وجد $0 \leq r < s$ حيث $m^{2^r t} \equiv -1 (\bmod n)$. الجهد الأساسي المبذول هنا هو إيجاد عدد حلول هذه التطابقات.

لنفرض أن $p - 1 = 2^i p'$ و $q - 1 = 2^j q'$ حيث p' و q' عددان فرديان. تذكر أن التطابق $ax \equiv b (\bmod n)$ قابل للحل إذا وفقط إذا كان $(a, n) \mid b$. وفي هذه الحالة يكون عدد الحلول غير المتطابقة قياس n يساوي (a, n) (تمرين (**١١,١,٢٠**)).

الحالة $m^t \equiv 1 (\bmod n)$:

ندرس أولاً التطابق قياس p. لنفرض أن $\alpha \in \mathbb{Z}_p^*$ مولّد. سنجد عدد الحلول x للتطابق $(\alpha^x)^t \equiv 1 (\bmod p)$.

(أ) أثبت أن p' يقسم t.

(ب) لاحظ أن:

$\alpha^{xt} \equiv 1 (\bmod p)$ إذا وفقط إذا كان $xt \equiv 0 (\bmod p - 1)$.

أثبت أن عدد الحلول يساوي p'.

(ج) بالمثل، عدد حلول التطابق $m^t \equiv 1 (\bmod q)$ يساوي q'. استخدم الآن مبرهنة الباقي الصينية لإثبات أن عدد حلول التطابق $m^t \equiv 1 (\bmod n)$ يساوي $p'q'$.

الحالة $m^{2^r t} \equiv -1 (\bmod n)$:

كما في الحالة السابقة نجد عدد الحلول قياس p ومن ثم عدد الحلول قياس q.
نسعى للحصول على عدد الحلول x للتطابق $(\alpha^x)^{2^r t} \equiv -1 (\bmod p)$.

(د) لاحظ أن $\alpha^{(p-1)/2} \equiv -1 (\bmod p)$. ولذا فإن $(\alpha^x)^{2^r t} \equiv -1 (\bmod p)$ إذا وفقط إذا كان $x 2^r t \equiv \frac{p-1}{2} (\bmod p-1)$. أثبت وجود حل للتطابق إذا وفقط إذا كان $r < i$. إضافة إلى ذلك أثبت أن عدد الحلول يساوي $2^r p'$.

نستطيع افتراض أن $i \le j$ دون المساس بالعمومية. الآن، نستخدم مبرهنة الباقي الصينية لإثبات أن عدد حلول التطابق $m^{2^r t} \equiv -1 (\bmod n)$ يساوي $2^{2r} p' q'$ إذا كان $r < i$ ويساوي صفراً ما عدا ذلك. الآن، الحد الأعلى لعدد الأعداد $m \in \mathbb{Z}_n^*$ التي تحقق $m^{2^r t} \equiv -1 (\bmod n)$ حيث $0 \le r < s$ هو:

$$\sum_{r=0}^{i-1} 2^{2r} p' q' = p' q' \left(2^{2i} - 1\right) / 3 .$$

وبهذا يكون الحد الأعلى لعدد الأعداد $m \in \mathbb{Z}_n^*$ التي تؤدي إلى فشل تحليل n هو:

$$p' q' \left(1 + \frac{2^{2i} - 1}{3}\right) = p' q' \left(\frac{2}{3} + \frac{2^{2i}}{3}\right) .$$

وبما أن:

$$2^{2i} p' q' \le 2^i p' 2^j q' = (p-1)(q-1) = \varphi(n)$$

فنجد أن:

$$p' q' \left(\frac{2}{3} + \frac{2^{2i}}{3}\right) \le \frac{\varphi(n)}{6} + \frac{\varphi(n)}{3} + \frac{\varphi(n)}{2} .$$

إذن، يوجد $1 \leq r \leq s$ لعلى الأقل نصف الأعداد $m \in \mathbb{Z}_n^*$ بحيث يكون:

$$m^{2^{r-1}} \not\equiv \pm 1 (\bmod n) \quad \text{و} \quad m^{2^r t} \equiv 1 (\bmod n).$$

لتحليل n، نقوم باختيار $m \in \mathbb{Z}_n^*$ عشوائياً ونجد r. بعد ذلك نقوم بحساب $\left(m^{2^{r-1}t} - 1, n\right)$. من المتوقع الحصول على قاسم غير تافه للعدد n بعد محاولتين.

(**١٢,٢,١٣**) إذا كان من المعلوم أن عملية التعمية $c \equiv m^e (\bmod pq)$ قد تمت عندما يكون $m \in \left[0, p\right)$ فمن الممكن إنجاز ذلك في المجموعة $\mathbb{Z}_p$ عوضاً عن المجموعة $\mathbb{Z}_{pq}$ وبهذا نحصل على النص الواضح كالتالي:

$$m \equiv c^d (\bmod n) \equiv c^{d \bmod (p-1)} (\bmod p).$$

اقترح شامير (Shamir [78]) نظام RSA غير متوازن حيث قام باختيار عددان أوليان $p < q$ من أطوال مختلفة تماماً، على سبيل المثال، طول p يساوي 500 مرتبة ثنائية وطول q يساوي 4500 مرتبة ثنائية. ويتم اختيار الرسائل الواضحة في الفترة $\left[0, p\right)$. وكانت نتيجة ذلك فشل محاولة كسر النظام بتحليل $n = pq$ وسرعة كشف المعمى في نظام RSA غير المتوازن مساوية لسرعة كشف المعمى في نظام RSA حيث طول القياس يساوي 500 مرتبة ثنائية. أثبت أنه يمكن كسر نظام RSA غير المتوازن تماماً بطريقة اختيار النص المعمى.

(**١٢,٢,١٤**) نشرت مجلة CRYPTO 96 [102] مقالاً بعنوان "جانب مظلم من صندوق أسود للتعمية". الفكرة الأساسية لهذا المقال هو افتراض تلوث صندوق أسود مع وجود تقنية تسمح للمُصَنِّع من الحصول على أسرار لا يمكن للآخرين من اكتشافها.

تعرف هذه التقنية باسم إخفاء معلومات سرية مع وجود حماية شاملة (Secretly Embedded Trapdoor with Universal Protection) أو اختصاراً SETUP. كان هدف المؤلفين المباشر لتقنية SETUP هو استخدامها على نظام RSA. الفكرة الأساسية لهذه الدراسة هو إخفاء معلومات كافية من قوة التعمية المعلنة e لنظام RSA بحيث تسمح للعدو من تحليل n. يختار الصندوق الأسود عددين أوليين $p \neq q$ ومن ثم يولد مفتاح تعمية $(n = pq, e, d)$ لنظام RSA. يتم تلويث العملية باستخدام مفتاح العدو (n', e') لمحاولة اختيار عدد أولي p حيث $e \equiv p^{e'} (\operatorname{mod} n')$ و $(e, \varphi(n)) = 1$.

(أ) ترك المؤلفين [102] بعض التفاصيل للقارئ. كيف يتمكن العدو من تحليل n باستخدام المفتاح المعلن (n, e) وما هي الفرضيات التي استخدمت لهذا الغرض؟

(ب) ناقش إمكانية اكتشاف SETUP مستنداً إلى الزمن اللازم لتوليد المفتاح أو شكل المفتاح المولَّد.

تقنية الـ SETUP المبينة أعلاه عديمة الفائدة في الحالات التي تكون فيها قوة التعمية e صغيرة. قدم المؤلفون خصوصية سيئة جداً (Pretty Awful Privacy) لتقنية SETUP مماثلة للخصوصية الجيدة جداً PGP (Pretty Good Privacy)، انظر [37,104]، ولكنهم أخفوا معلومات عن p في عدد القياس n. انظر أيضاً [103] والتمرين (**١٢,٥,٦**).

(١٢,٣) الأمن القابل للبرهان

Provable Security

يعتمد أمن نظام RSA على فرضية صعوبة مسألة تحليل الأعداد ومع ذلك تبين أن المحاولة المستمرة والمنظمة للحصول على النص الواضح من النص المعمى في نظام RSA

ليس معلوماً أن صعوبتها تكافئ صعوبة مسألة التحليل. ولذا فمن المحتمل أن تكون مسألة تحليل الأعداد مسألة صعبة ولكن كسر نظام RSA مسألة سهلة.

قدم رابن (Rabin [69]) في العام ١٩٧٩م نظام تعمية يمكن إثبات أنه آمن، وهذا يعني أن صعوبة الحصول على النص الواضح من نص معمى تكافئ مسألة حسابية يعتقد عدم وجود خوارزمية فعالة لحلها. إن الأمن القابل للبرهان يقلل من الفرضيات ويقدم لنا تعريفاً أكثر دقة لمفهوم الأمن. يجب توضيح نقطة مهمة هنا وهي أن البرهان يفترض صعوبة المسألة الحسابية ذات العلاقة فمن الممكن وجود معلومات مقنعة بصعوبة حل مسائل حسابية مثل مسألة التحليل أو مسألة اللوغاريتم المنفصل ولكن لم يتم تقديم برهان ذلك حتى الآن.

نظام رابن يشبه نظام RSA حيث دالة التعمية في كلا النظامين هي على الصورة $f(m) \equiv m^e (\bmod pq)$. في نظام RSA تكون هذه الدالة قابلة للعكس وأما نظام رابن فيستخدم $e = 2$ ، ومن ثم فحساب الجذور التربيعية يقدم لنا الخيارات الممكنة للرسالة m . والتعريف الدقيق لنظام رابن يتم باختيار عددين أوليين $p \neq q$ ويكون المفتاح المعلن هو $n = pq$ والمفتاح السري هو (p, q). دالة التعمية هي $f : \mathbb{Z}_n \to \mathbb{Z}_n$ ومعرفة بالقاعدة:

$$f(m) \equiv m^2 (\bmod n) .$$

إذا كان c نصاً معمى فيتم كشف المعمى بحل التطابق $c \equiv m^2 (\bmod n)$ لإيجاد الجذور التربيعية الأربعة كما هو مبين في البند (**١١,٤**).

مثال (١٢,٣,١)

لنفرض استخدام $p = 31$ و $q = 41$ في نظام رابن. لتعمية الرسالة $m = 814$ باستخدام المفتاح المعلن $n = pq = 1271$ نحصل على النص المعمى:

$$c = f(m) \equiv m^2 \equiv 814^2 \equiv 405 (\bmod 1271) .$$

ولكشف المعمى نستخدم المفتاح السري $p = 31$ و $q = 41$ لإيجاد الجذور التربيعية. ولقد بينا في البند (**١١,٤**) وجود خوارزمية فعالة لحل التطابقين:

$$m^2 \equiv 405 \equiv 2 \pmod{31}$$
$$m^2 \equiv 405 \equiv 36 \pmod{41}$$

وإيجاد الجذور التربيعية m. لاحظ أن $p \equiv 3 \pmod 4$. ولذا نجد أن الجذرين التربيعيين قياس p هما:

$$m \equiv \pm 2^{(p+1)/4} \equiv \pm 8 \pmod{31}.$$

أما الجذران التربيعيان قياس $q = 41$ فأحدهما سهل لأن 36 مربع كامل. وبهذا نجد:

$$m \equiv \pm 6 \pmod{41}$$

الآن، نستخدم خوارزمية جاوس (**١١,١,٦**) ونحصل على الجذور التربيعية الأربعة m_1 ، m_2 ، m_3 ، m_4 بحل كل من أنظمة التطابقات التالية:

$$\left\{\begin{array}{l} m \equiv 8 \pmod{31} \\ m \equiv 6 \pmod{41} \\ m_1 = -240 \end{array}\right\} \quad ، \quad \left\{\begin{array}{l} m \equiv -8 \pmod{31} \\ m \equiv 6 \pmod{41} \\ m_2 = 457 \end{array}\right\}$$

$$\left\{\begin{array}{l} m \equiv 8 \pmod{31} \\ m \equiv -6 \pmod{41} \\ m_3 = -457 \end{array}\right\} \quad ، \quad \left\{\begin{array}{l} m \equiv -8 \pmod{31} \\ m \equiv -6 \pmod{41} \\ m_4 = 240 \end{array}\right\}.$$

(لاحظ أننا نحتاج فقط لحل النظامين الأول والثاني لأن الجذور هي $\pm m_1$ و $\pm m_2$).

وبهذا نحصل على أربعة خيارات مختلفة m_i للنص الواضح m. وبحالة عدم تذيل الرسالة بمعلومات إضافية قبل تعميتها فيكون من الصعب على المستقبل أن يخمن الرسالة الواضحة على أنها:

$$m_3 \equiv 814 \pmod n. \qquad \blacktriangle$$

لفهم أمن النظام نقدم مسألة رابن وهي المهمة بالنسبة للعدو.

مسألة رابن (RABIN): لنفرض أن $n = pq$ وأن $c \equiv m^2 (\bmod n)$. جد x يحقق $c \equiv x^2 (\bmod n)$.

هذه هي مسألة الجذور التربيعية التي قدمناها في البند (**٤,١١**). إذا كان $p \equiv q \equiv 3 (\bmod 4)$ فإن العدد $n = pq$ هو عدد بلم ومن ثم يمكن إيجاد الجذور التربيعية بزمن حدودي. في المثال أعلاه، $q \equiv 1 (\bmod 8)$. ولهذا فالعدد n ليس على الصيغة المطلوبة. لا توجد خوارزمية حدودية معلومة لحل التطابق $x^2 \equiv c (\bmod q)$ عندما يكون $q \equiv 1 (\bmod 8)$. ولكن توجد طريقة عشوائية ناقشناها في البند (**٤,١١**) زمن تنفيذها المتوقع حدودي. إذن، RABIN ≤ FACTOR. أي إذا وجدت خوارزمية زمن تنفيذها لتحليل العدد حدودي فمن الممكن حل مسألة رابن بزمن متوقع حدودي. ولبرهان العكس، أي برهان FACTOR ≤ RABIN، تذكر أولاً أنه إذا كان $x^2 \equiv y^2 (\bmod n)$ وكان $x \not\equiv \pm y (\bmod n)$ فإن $(x + y, n)$ قاسم غير تافه للعدد n. الآن، اختر $x \in \mathbb{Z}_n^*$ عشوائياً واحسب $c \equiv x^2 (\bmod n)$. استخدم خوارزمية حساب رابن لإيجاد جذر تربيعي y للعدد c بزمن متوقع حدودي. احتمال أن يحقق y العلاقة $y \not\equiv \pm x$ يساوي $\frac{1}{2}$. وبهذا يكون $(x + y, n)$ قاسم غير تافه للعدد n (أي أحد العددين الأوليين).

إذن، نخلص إلى أن كسر نظام رابن يكافئ تحليل n. لاحظ أن البرهان السابق لا يضمن أمن النظام ضد محاولة كسره باختيار النص المعمى. إضافة إلى ذلك من الممكن تطبيق اتفاقية من النمط المبين في التمرين (**٤,٢,١٢**) على نظام رابن.

إحدى صعوبات كشف المعمى في نظام رابن هو صعوبة تخمين النص الواضح الصحيح من بين الأربعة نصوص (الجذور التربيعية). وللتغلب على هذه الصعوبة، عادة يتم تذيل الرسالة الواضحة قبل تعميتها بمعلومات إضافية (مثل تكرار بعض مراتبها) بطريقة يكون فيها من الصعب تحقيق أكثر من جذر من الجذور الأربعة لهذه

الخاصية. وهذه الطريقة تصلح أيضاً لمقاومة محاولة كسر النظام باختيار النص المعمى (لأن مخرج الخوارزمية لا يقدم معلومات مفيدة للعدو في هذه الحالة). ولكن برهان التكافؤ بين مسألة رابن ومسألة التحليل غير مضمونة في هذا النظام المعدل. يقدم التمرين (**١٢,٣,٣**) نظام شبيه بنظام رابن (على أعداد بلم) حيث يضمن هذا النظام معرفة الرسالة الأصلية.

تمارين

(**١٢,٣,٢**) ليكن $n = 551$ هو القياس في نظام رابن.

(أ) جد النص المعمى $c \equiv m^2 (\bmod n)$ للرسالة $m = 53$.

(ب) جد النص الواضح للرسالة المعماة c بالحصول على الجذور التربيعية الأربعة المرشحة بأن تكون الرسالة m .

(ج) ناقش محاولة كسر النظام باختيار النص المعمى على النحو التالي:
اختار $x \in \mathbb{Z}_{551}^*$ عشوائياً وليكن $x = 53$. أدخل القيمة $c \equiv x^2 (\bmod n)$ إلى خوارزمية RABIN. ماذا يحدث لو كان مخرج الخوارزمية 498 ؟ إذا كان مخرج الخوارزمية هو 517 فأثبت أن باستطاعتك تحليل n .

(**١٢,٣,٣**) يقدم هذا التمرين الشكل العام لنظام تعمية طرحه وليامز ([96, 97] Williams) لعدد مؤلف مختار n وهو نظام شبيه بنظام رابن حيث الحصول على النص الواضح من النص المعمى يكافئ تحليل العدد n ولكن يسمح بمعرفة النص الواضح الأصلي من بين الجذور التربيعية الأربعة.

افرض أن $n = pq$ حيث $p \equiv q \equiv 3 (\bmod 4)$ وأن:

$d = \big((p-1)(q-1) \,/\, 4 + 1\big) \,/\, 2$.

اختر s يحقق $\left(\dfrac{s}{n}\right) = -1$. المفتاح المعلن هو (n, s) والمفتاح السري هو d .

التعمية: اختر رسالة m حيث $(m,n)=1$. احسب $b_1 \in \{0,1\}$ بحيث يكون $(-1)^{b_1} = \left(\frac{m}{n}\right)$ واحسب $m_0 \equiv s^{b_1} m (\bmod n)$. أرسل الثلاثي:

$\left(c \equiv m_0^2 (\bmod n), b_1, b_2 \equiv m_0 (\bmod 2)\right)$.

كشف المعمى: عند استلامك للثلاثي (c, b_1, b_2)، احسب $m_0 \equiv \pm c^d (\bmod n)$ حيث تختار الإشارة التي تحقق $m_0 \equiv (-1)^{b_2} (\bmod 2)$. عندئذ، الرسالة الواضحة هي $m \equiv s^{-b_1} m_0 (\bmod n)$.

(أ) إذا كان $\left(\frac{x}{n}\right) = 1$ و $c \equiv x^2 (\bmod n)$ فأثبت أن $c^d \equiv \pm x (\bmod n)$.

(ب) تحقق من الحصول بالفعل على الرسالة m بإجراء كشف المعمى.

(ج) افرض أن $p = 7$، $q = 11$، $n = pq$. لاحظ أن $p \equiv q \equiv 3 (\bmod 4)$. أثبت أن $s = 2$ تحقق $\left(\frac{s}{n}\right) = -1$. وضح التعمية وكشف المعمى للرسالة $m = 31$.

السمة الأساسية لهذا النظام هو تمييز الجذر التربيعي الصحيح (من بين الأربعة جذور تربيعية) في حالة $n = pq$ حيث $p \equiv q \equiv 3 (\bmod 4)$. سنستخدم الترميز نفسه الذي استخدمه وليامز في بحثه. افرض أن $[a,b]$ يرمز لفصل الرواسب قياس n بحيث يتحقق ما يلي: إذا كان $y \in [a,b]$ فإن $y \equiv a (\bmod p)$ و $y \equiv b (\bmod q)$.

(د) أثبت أن $\left(\frac{-1}{p}\right) = -1$. استنتج من ذلك أنه إذا كان $(c,p) = 1$ فإن واحداً فقط من بين العددين $\pm c$ هو راسب تربيعي قياس p.

(هـ) إذا كان $(y,n) = 1$ فأثبت إمكانية كتابة الجذر التربيعي للعدد y^2 في $\mathbb{Z}_n$ على الصور $[a,b]$، $[-a,-b]$، $[-a,b]$، $[a,-b]$ حيث $a \in Q_p$ و $b \in Q_q$.

(و) إذا كان $y \in [a,b]$ أو $y \in [-a,-b]$ فنقول إن y هو جذر تربيعي للعدد y^2 من النمط 1 ونقول إن باقي الجذور التربيعية هي من النمط 2. أثبت أن y من النمط 1 إذا وفقط إذا كان $\left(\frac{y}{n}\right) = 1$. ومن ثم فالتحليل ليس ضروري لمعرفة النمط.

(ز) إذا كان y_1 و y_2 جذرين مختلفين من النمط 1 فأثبت أن $y_1 \equiv -y_2 (\bmod n)$ وأن واحداً فقط منهما زوجي.

العدو الذي لديه القدرة على كشف المعمى يحصل على جذر تربيعي من النمط 1 وآخر من النمط 2 لعدد مختار ومن ثم يكون باستطاعته تحليل n.

(ح) يجد العدو عدد x يحقق $\left(\frac{x}{n}\right) = -1$ ثم يطبق عملية كشف المعمى على x^2.

إذا تمكن من كشف معمى كل نص من النصوص المعماة الصحيحة فعندئذ يمكن اختيار $s = x$. يقوم العدو الآن بكشف المعمى $\left(x^2, 0, 0\right)$ ويحصل على جذر تربيعي y من النمط 1. أثبت أن $(y-x, n)$ هو قاسم غير تافه للعدد n.

(١٢,٤) نظام الجمل
ELGamal Cipher

قدم الجمل ([29] ELGamal) في العام ١٩٨٥م نظام تعمية وخطة توقيع إلكتروني يعتمدان على فرضية صعوبة حل مسألة اللوغاريتم المنفصل. وكان توقيع الجمل هو أول توقيع تتبناه الحكومة الأمريكية في العام ١٩٩٤م حيث التوقيع الإلكتروني القياسي (Digital Signature Standard) أو اختصاراً DSS هو صيغة معدلة لخطة توقيع الجمل.

تحتاج عملية التعمية في نظام الجمل إلى عدد أولي p ومولداً $\alpha \in \mathbb{Z}_p^*$. يختار كل مستخدم عدداً عشوائياً a حيث $1 \leq a \leq p-2$ كمفتاح سري ويكون المفتاح

المعلن هو $\left(p,\alpha,\alpha^{a}(\bmod p)\right)$. لإرسال رسالة m حيث $0 \le m < p$ باستخدام المفتاح المعلن يقوم المرسل باختيار عشوائي لعدد k حيث $1 \le k < p$ ثم يرسل الزوج المرتب $\left(\alpha^{k}(\bmod p), m\left(\alpha^{a}\right)^{k}(\bmod p)\right)$. وباستخدام المفتاح السري a يمكن كشف المعمى وإيجاد الرسالة m ؛ لأنه يمكن حساب α^{-ak}. وبهذا يكون $m\left(\alpha^{a}\right)^{k}\alpha^{-ak} \equiv m(\bmod p)$.

مثال (١٢,٤,١) (مثال صفي على تعمية الجمل)

ليكن $p = 13$. وليكن $\alpha = 2 \in \mathbb{Z}_{13}^{*}$ مولّداً. يمكن اختيار المفتاح المعلن a حيث $1 \le a \le 13-2$. لنفرض أن أليس اختارت $a = 6$. تقوم أليس بحساب:

$$\alpha^{a} \equiv 2^{6} \equiv 12(\bmod 13)$$

ومن ثم تعلن عن $\left(p,\alpha,\alpha^{a}(\bmod p)\right) = (13,2,12)$ كمفتاح معلن. لإرسال الرسالة $m = 9$ يختار بوب عدد عشوائي k حيث $1 \le k < p$ وليكن $k = 3$. وباستخدام مفتاح أليس المعلن يقوم بوب بإرسال:

$$\begin{aligned}(\gamma,\delta) &= \left(\alpha^{k}(\bmod p), m\left(\alpha^{a}\right)^{k}(\bmod p)\right)\\ &\equiv \left(2^{3}, 9(12)^{3}\right) \equiv (8,4)(\bmod 13)\end{aligned}$$

إلى أليس. بعد ذلك تستطيع أليس استخدام مفتاحها السري $a = 6$ لقراءة الرسالة وذلك بحساب:

$$\left(\alpha^{k}\right)^{-a} \equiv \gamma^{-a} \equiv \gamma^{p-1-a} \equiv 8^{13-1-6} \equiv 12(\bmod 13)$$

وبهذا تكون الرسالة هي:

$$.\, m \equiv \delta\alpha^{-ak} \equiv 4 \cdot 12 \equiv 9(\bmod 13)$$

لاحظ أن توليد المفتاح في هذا المثال يؤدي إلى أن $\alpha^{a} \equiv -1(\bmod p)$ وهذا غير مفضل كما هو موضح في التمرين (**١٢,٤,٥**). ▲

إحدى نقاط قوة نظام الجمل هو وجود عشوائية صريحة في عملية التعمية ومن ثم فالرسالة m يمكن أن تعمى إلى نصوص معماة مختلفة اعتماداً على الاختيار

العشوائي للعدد k. ومن ثم يكون النظام محمياً ضد بعض محاولات كسره. لاحظ أننا سبق وأن أدخلنا العشوائية على نظام شبيه لنظام RSA وحصلنا على الحماية نفسها. أما إحدى نقاط ضعف نظام الجمل فهو تمديد سعة الرسالة؛ لأن النص المعمى يتكون من زوج من الأعداد الصحيحة كل منها يساوي تقريباً الرسالة.

المسألة التالية تهم العدو:

مسألة الجمل (ELGAMAL): ليكن p عدداً أولياً وليكن $\alpha \in \mathbb{Z}_p^*$ مولّداً إذا علمت α^a ، α^k ، $m\left(\alpha^a\right)^k$ فجد m.

من الواضح أن وجود خوارزمية حدودية لحل مسألة اللوغاريتم المنفصل يؤدي إلى وجود خوارزمية حدودية لحل مسألة ELGAMAL. أي أن $\text{ELGAMAL} \le \text{DLP}$. ولذا فأمن نظام الجمل يعتمد على مسألة اللوغاريتم المنفصل ولكن ليس من المعلوم أن مسألة ELGAMAL تكافئ مسألة DLP.

لاحظ أن التبديل بين α^a و α^k هو جزء من اتفاقية ديفي وهيلمان للحصول على مفتاح مشترك α^{ak}. ومن ثم يستخدم نظام الجمل هذا المفتاح المشترك لتعمية الرسالة m بضربها بهذا المفتاح. ولذا فإن وجود خوارزمية لحل مسألة ديفي وهيلمان يؤدي مباشرة إلى حل مسألة الجمل. أي أن $\text{ELGAMAL} \le \text{DHP}$. ولبرهان أن $\text{DHP} \le \text{ELGAMAL}$ نفرض وجود خوارزمية حدودية لحل مسألة الجمل. أي إذا كان لدينا $\left(p, \alpha, \alpha^a, \alpha^k, m\alpha^k\right)$ فنستطيع الحصول على مخرج الخوارزمية m بزمن حدودي. وفي مسألة ديفي وهيلمان يكون المطلوب إيجاد α^{ak} بمعرفة $\left(p, \alpha, \alpha^a, \alpha^k\right)$. ولذا بإدخال $\left(p, \alpha, \alpha^a, \alpha^k, 1\right)$ إلى خوارزمية الجمل نحصل على المخرج $m = \alpha^{-ak}$. وبعد ذلك نقوم بأخذ النظير (يحتاج ذلك إلى زمن حدودي) ونحصل على α^{ak}.

توقيع الجمل

تستخدم خطة توقيع الجمل دالة تمويه بحيث تكون صورة الرسالة m التي يمكن أن يكون طولها كبيراً جداً هي ملخص الرسالة x ومن ثم يتم توقيع x. يحتاج التحقق من صواب التوقيع إلى وجود الرسالة نفسها. ولهذا فخطة توقيع الجمل هي مثال على التوقيع بملحق.

يتم توليد المفتاح لغرض التوقيع بصورة مماثلة لتوليد مفتاح التعمية. لنفرض أن الرسالة المراد توقيعها هي $m \in \{0,1\}^*$. نستخدم دالة تمويه معروفة $H : \{0,1\}^* \to \{0, \ldots, p-1\}$ للحصول على ملخص الرسالة $x = H(m)$. يتم اختيار عدد عشوائي k، $1 \leq k < p$ حيث $(k, p-1) = 1$. يتم حساب $r \equiv \alpha^k (\mathrm{mod}\, p)$.
نستخدم الآن المفتاح السري a لحل التطابق:

$$x \equiv ar + ks (\mathrm{mod}\, p - 1)$$

لإيجاد s. توقيع الرسالة m هو الزوج (r, s).

يتم التحقق من صواب التوقيع من المفتاح المعلن باستخدام الحقيقة:

$$\alpha^x \equiv \alpha^{ar+ks} \equiv \left(\alpha^a\right)^r \left(\alpha^k\right)^s (\mathrm{mod}\, p)$$

لنفرض أن (r, s) هو التوقيع المزعوم على الرسالة m. نقوم باستخدام دالة التمويه المعروفة لحساب $x = H(m)$. يتم قبول التوقيع إذا تحقق $\alpha^x \equiv \left(\alpha^a\right)^r \left(\alpha^k\right)^s (\mathrm{mod}\, p)$ حيث $1 \leq r < p$. (انظر التمرين (**١٢,٤,٣**)).

إذا حاول العدو تزوير التوقيع على الرسالة m فإنه يقوم بحساب $x = H(m)$ و $r = \alpha^k$ لأي k. ولكنه لا يستطيع إيجاد قيمة a و s بحل التطابق $x \equiv ar + ks (\mathrm{mod}\, p - 1)$ ولكن من الممكن إيجاد x وتوقيع (r, s) بحيث يكون شرط التحقق:

$$\alpha^x \equiv \left(\alpha^a\right)^r \left(\alpha^k\right)^s (\mathrm{mod}\, p)$$

صحيحاً. ولإنجاز ذلك نقوم باختيار عددين صحيحين j و k حيث $1 \leq k < p$ و $(k, p-1) = 1$ وحساب:

$$r \equiv \alpha^{j}\left(\alpha^{a}\right)^{k} (\bmod p)$$
$$s \equiv -rk^{-1}(\bmod p-1)$$
$$x \equiv sj(\bmod p-1)$$

وبهذا يكون التوقيع (r,s) على x صائباً لأن:

$$\left(\alpha^{a}\right)^{r} r^{s} \equiv \alpha^{ar}\alpha^{js}\alpha^{aks} \equiv \alpha^{js} \equiv \alpha^{x}(\bmod p)$$

وبهذا يتم قبول التوقيع إذا استطاع العدو إيجاد رسالة m حيث $H(m) = x$. يسمى كشف المعمى هذا بالتزوير الوجودي (existential forgery)؛ لأن المعلومات التي يعرفها العدو عن محتوى الرسالة قليلة جداً.

إحدى الوسائل الأخرى التي يحاول العدو استخدامها لكسر خطة توقيع الجمل هو حل التطابق:

$$\alpha^{x} \equiv \left(\alpha^{a}\right)^{r} r^{s}(\bmod p)$$

للتوقيع (r,s). من الواضح أن ذلك ممكناً إذا استطاع العدو معرفة المفتاح السري a (ربما من توقيع سابق معلوم). ولكن معرفة a من معلومات معلنة يكافئ مسألة اللوغاريتم المنفصل. وحل s بدلالة r هي أيضاً مسألة اللوغاريتم المنفصل. وأما محاولة حل r بدلالة s تؤدي إلى تطابق أسي في r ولا توجد خوارزمية فعالة لحل مثل هذا التطابق.

لضمان أمن النظام يجب أن يكون العدد الأولي p كبيراً جداً بحيث يتعذر حل مسألة اللوغاريتم المنفصل في الزمرة $\mathbb{Z}_p^*$. في العام ١٩٩٦م لاحظ مينيزس [63] أن استخدام عدد أولي p طوله 512 مرتبة ثنائية ليس آمناً واقترح الطول 768. وإذا أردنا أمن طويل الأجل فاقترح أن يكون طول العدد الأولي يساوي 1024 مرتبة ثنائية.

لاحظ أيضاً أن طول التوقيع هو ضعف طول العدد الأولي مما يعيق استخدامه في بعض التطبيقات مثل البطاقة الذكية.

استخدمت صورة معدلّة لتوقيع الجمل في التوقيع الإلكتروني القياسي (DSS) في العام ١٩٩٤م. وعلى الرغم من أن طول القياس p يتراوح بين 512 و 1024 مرتبة ثنائية ، إلا أنه من الممكن استخدام توقيع طوله 320 مرتبة ثنائية نحصل عليه من تمويه طوله 160 مرتبة ثنائية باستخدام زمرة جزئية من $\mathbb{Z}_p^*$. انظر [63] للحصول على تفاصيل خوارزمية التوقيع الإلكتروني (DSA) وخوارزمية التمويه الآمن (SHA-1) المستخدمة كدالة تمويه.

يستخدم توليد مفتاح DSA عدداً أولياً q طوله 160 مرتبة ثنائية وعدد أولي p حيث $q \mid (p-1)$ بحيث يكون طول p يساوي $512 + 64t$ مرتبة ثنائية ، $0 \leq t \leq 8$ (بحد أقصى 1024 مرتبة ثنائية). لنفرض أن β مولّداً للزمرة الجزئية الدورية من الرتبة q من $\mathbb{Z}_p^*$ (انظر التمرين (**١٢,٤,٤**)). يتم اختيار مفتاح سري a عشوائياً حيث $1 \leq a < q$. المفتاح المعلن هو $\left(p, q, \beta, \beta^a (\bmod p)\right)$.

لتوقيع رسالة m نجد التمويه $x = H(m)$ الذي طوله 160 مرتبة ثنائية. يتم اختيار عدد k عشوائياً حيث $1 \leq k < q$. وبعد ذلك يتم حساب التوقيع (r, s) على النحو التالي :

$$s \equiv (x + ar)^{-1} k (\bmod q) \quad \text{و} \quad r \equiv \left(\beta^k (\bmod p)\right) (\bmod q)$$

يتم قبول (r, s) كتوقيع صائب للرسالة m إذا تحقق ما يلي :

$$\left(\beta^{xs^{-1} (\bmod q)} \left(\beta^a\right)^{rs^{-1} (\bmod q)} (\bmod p)\right) (\bmod q) \equiv r$$

(انظر التمرين (**١٢,٤,٤**)).

تمارين

(**١٢,٤,٢**) مثال صفي على توقيع الجمل. لنفرض أن أليس اختارت $p = 17$ والمولّد $\alpha = 3 \in \mathbb{Z}_{17}^*$ والمفتاح السري $a = 6$.

المفتاح المعلن هو $\left(p, \alpha, \alpha^a (\bmod p)\right) = (17, 3, 15)$. دالة التمويه هي $H(m) \equiv m (\bmod p)$.

(أ) جد قيمة التمويه x والتوقيع (r, s) للرسالة $m = 26$ بفرض أن أليس اختارت $k = 11$ (لاحظ أن $(k, p-1) = 1$).

(ب) بين تفاصيل التحقق من صواب التوقيع (r, s) على m مع توضيح عدم الحاجة إلى معرفة المفتاح السري a.

(**١٢,٤,٣**) إذا لم يتم التحقق من الشرط $1 \leq r < p$ أثناء التحقق من صواب توقيع الجمل فيكون بالإمكان تزوير التوقيع على رسالة m' مع وجود شرط صواب التوقيع (r, s) على قيمة تمويه x حيث $(x, p-1) = 1$. في هذه الحالة نفرض أن $x' = H(m')$ وأن $u \equiv x' x^{-1} (\bmod p - 1)$. ضع $s' \equiv su (\bmod p - 1)$ واستخدم مبرهنة الباقي الصينية لحل النظام:

$$r' \equiv ru (\bmod p - 1)$$
$$r' \equiv r (\bmod p)$$

لإيجاد قيمة r'. أثبت أن (r', s') توقيع مقبول للرسالة m' إذا تجاهلنا الشرط $1 \leq r' < p$ (أُخذ هذا التمرين من [10]، انظر أيضاً [63] الملحوظة (**١١,٦٦**)).

(**١٢,٤,٤**) يناقش هذا التمرين تفصيلان من تفاصيل خوارزمية التوقيع الإلكتروني.

(أ) لنفرض أن $g \in \mathbb{Z}_p^*$ يحقق $\beta \equiv g^{(p-1)/q} (\bmod p) \neq 1$. أثبت أن رتبة β تساوي q.

(ب) إذا كان $s \neq 0$ فأثبت صواب التحقق من التوقيع.

(١٢,٤,٥) في المثال (**١٢,٤,١**) حصلنا من توليد المفتاح على التطابق $\alpha^a \equiv -1 (\bmod p)$. لماذا كان هذا الاختيار سيئاً؟ [إرشاد: ما هي قيمة $m\left(\alpha^a\right)^k$ لكل خيار للعدد k ؟].

(١٢,٤,٦) (مولدات ضعيفة) لنفرض أن $p \equiv 1 (\bmod 4)$ وأن $\alpha \in \mathbb{Z}_p^*$ مولّد يحقق $\alpha \mid (p-1)$. إذا كان حساب اللوغاريتمات في زمرة جزئية G من $\mathbb{Z}_p^*$ رتبتها α ممكناً فيكون بإمكان العدو إنشاء توقيع (r,s) على رسالة m على النحو التالي:

لنفرض أن مفتاح أليس المعلن هو α^a وأن r معرفاً بحيث يحقق $p-1=\alpha r$.

(أ) أثبت أن α^r مولّد للزمرة G . وبهذا يكون من الممكن إيجاد z يحقق $\alpha^{rz} \equiv \left(\alpha^a\right)^r (\bmod p)$.

(ب) أثبت أن $r^{(p-1)/2} \equiv -1 (\bmod p)$.

(ج) افرض أن $s \equiv \dfrac{p-3}{2}(H(m)-rz)(\bmod p-1)$. أثبت أن (r,s) توقيعاً مقبولاً على الرسالة m .

(١٢,٤,٧) إعادة استخدام العدد العشوائي k في نظام الجمل يؤدي إلى مخاطر.

(أ) لنفرض أن k استخدم لتعمية الرسالتين m_1 و m_2 .

أثبت أن حيازة العدو على النصين المعميين والرسالة $m_1 \neq 0$ يؤدي إلى معرفة الرسالة m_2 بطريقة فعالة.

(ب) لنفرض أن k استخدم لتوقيع الرسالتين m_1 و m_2 .

أثبت إمكانية معرفة العدو للمفتاح السري a .

(١٢,٥) بروتوكولات (معاهدات أو اتفاقيات) تعموية
Cryptographic Protocols

البروتوكول أو المعاهدة أو الاتفاقية هو هيكل عام من الإجراءات لتطبيق المفاهيم البدائية للتعمية. التعريف المقدم في [25] للبروتوكول هو "خوارزمية لتنفيذ صنف من التعاملات (وحدات منطقية لتنشيط الاتصال)". نقدم في هذا البند القصير عدة مفاهيم لها علاقة بالبروتوكولات حيث نناقش مسألتين تقليديتين هما :

برتوكول رمي قطعة نقود بين فريقين حيث كل منهما لا يثق في الآخر ويرغبان في حل خلاف بينهما برمي قطعة نقود باستخدام الهاتف. أما برتوكول عدم المعرفة مطلقاً (Zero-Knowledge) فيقدم برهاناً على حوزة أحدهم على سر دون إفشاء أي معلومة عن ذلك السر.

يبين الهجوم النشط على خطة ديفي وهيلمان لتبادل المفاتيح الحاجة إلى توضيح فرضيات البرتوكول. وحتى مع أن فرضيات البرتوكول واضحة فإنه ليس من المعلوم ما إذا كانت هذه الفرضيات تلبي المطلوب عند دراسة حالة معينة. ومثال على ذلك هو برتوكول لعبة البوكر الذهنية (لعبة بوكر عادلة (غير متحيزة) دون استخدام ورق اللعب) التي قدمها كل من شامير ورايفست وأدلمان في [79] حيث تبين لاحقاً أنها تقدم معلومات كافية للحصول على تعليم جزئي لأوراق اللعب.

عند اكتشاف ضعف في الأمن فإنه ليس من الواضح دائماً اكتشاف السبب ، هل هو من البرتوكول أو من دالة التعمية. كتب مور (Moore [64]) : "عند اكتشاف ضعف في نظام تعمية فيجب علينا التفريق بين أمرين فإذا كانت النتيجة لهذا الاكتشاف هي الحد من مدى التطبيقات أو تحديد مدى المتغيرات التي يجب استخدامها في الخوارزمية فمن الممكن أن يكون سبب هذا الضعف هو فشل البرتوكول. أما إذا كان تأثير هذا الاكتشاف هو عدم الصلاحية الكاملة للنظام المستخدم أو قصر مدى المتغيرات المستخدمة

بشكل مجحف بحيث يجعل دالة التعمية صعبة الحساب فيكون نظام التعمية قد تم كسره فعلياً." ولذا فالضعف المقدم في التمرين (**١٢,٢,٤**) هو نتيجة فشل البرتوكول حسب إدعاء مور. وفي التمرين (**١٠,٣,٨**) تم الدمج بين نظامين آمنين حيث تمت مقايضة بين التعمية والتوثيق. ولذا يمكن الجدال على أن هذا هو فشل في البرتوكول مع أن مقولة مور تدعى أن هذا هو كسر لنظام التعمية.

برتوكول الثلاث خطوات لشامير

يوضح برتوكول الثلاث خطوات لشامير الفرق بين البرتوكول والدالة التعموية. صمم شامير هذا البرتوكول للحصول على السرية دون التبادل المسبق للمفاتيح. يتم اختيار نظام تعمية تقليدي (متماثل المفتاح) يحقق الخاصية $E_{k_1}E_{k_2} = E_{k_2}E_{k_1}$ لكل $k_1, k_2 \in \mathcal{K}$. من الممكن النظر إلى عملية التعمية على أنها تضع "قفلاً" على الصندوق الذي يحتوي الرسالة. الخطوات التالية توضح البرتوكول لغرض إرسال رسالة m من A إلى B.

(١) يختار كل من A و B عشوائياً مفتاح سري K_A و K_B على التوالي.

(٢) تضع A قفلها على الرسالة وترسل $c_1 = E_{k_A}(m)$ إلى B.

(٣) يقوم B بوضع قفله و إعادة $c_2 = E_{k_B}(c_1) = E_{k_B}E_{k_A}(m)$ إلى A.

(٤) تقوم A بإزالة قفلها وترسل $c_3 = D_{k_A}(c_2)$ إلى B. يكشف B المعمى c_3 ليحصل على الرسالة m.

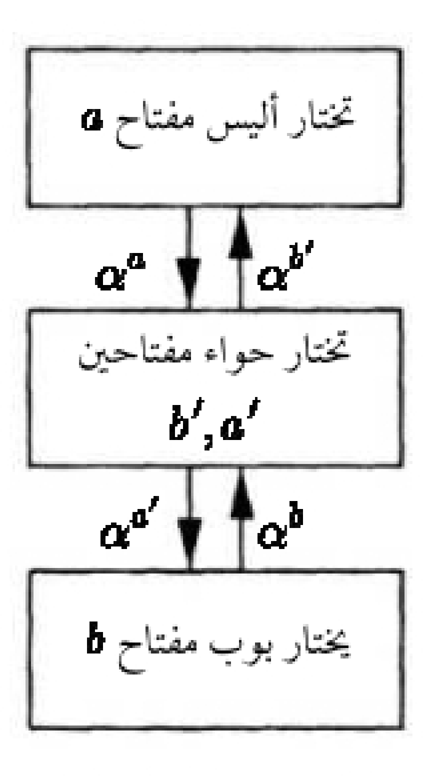
بوضع شروط مناسبة على E، يبدو أن هذا التبادل مقاوماً لمحاولات الكسر. ولكن البرتوكول يضع شروطاً إضافية ضمنية على نظام التعمية. لنأخذ الحالة التي يكون فيها النظام هو نظام اللفافة للمرة الواحدة. عندئذ، $E_k(m) = k \oplus m$. إذا حصل العدو على:

$$c_1 = k_A \oplus m \quad ، \quad c_2 = k_B \oplus c_1 \quad ، \quad c_3 = k_B \oplus m$$

فنجد أن التبادل غير آمن على الإطلاق ؛ لأن $c_1 \oplus c_2 \oplus c_3 = m$. هذا مع أن النظام المستخدم في البرتوكول آمن تماماً. يقترح التمرين (**١٢,٥,١**) نظاماً آخر لاستخدامه في هذا البرتوكول.

(١٢,٥,١) اتفاقية ديفي وهيلمان لتبادل المفاتيح

في اتفاقية ديفي وهيلمان لتبادل المفاتيح المقدمة سابقاً يقوم أليس وبوب بتبادل $\alpha^a \pmod p$ و $\alpha^b \pmod p$ من خلال قناة اتصال مفتوحة (غير آمنة) للحصول على المفتاح السري المشترك α^{ab} . هذه الخطة آمنة ضد الهجوم السلبي ولكنها غير آمنة ضد الهجوم الإيجابي (النشيط).



الاعتراض في المنتصف

إذا لم تكن المفاتيح موثقة فبإمكان العدو النشط إضافة إلى انتحال الشخصية أن يصمم هجوم يدعى اعتراض في المنتصف (intruder-in the middle) بحيث لا يستطيع أي من أليس أو بوب اكتشافه. ويتم ذلك بأن تشارك حواء (العدو) السر $\alpha^{ab'}$ مع أليس و السر $\alpha^{a'b}$ مع بوب حيث a' و b' مختاران من قبل حواء. إذا أرسلت أليس رسالة معماة باستخدام مفتاح مشتق من $\alpha^{ab'}$ ، تقوم حواء باعتراض الرسالة وتكشف المعمى ثم تعيد التعمية باستخدام مفتاح مشتق من $\alpha^{a'b}$ وترسلها إلى بوب. وبهذا يكون بمقدور حواء الحصول على جميع النصوص الواضحة المتبادلة[٤].

يستعان أحياناً بمصدر مؤتمن أو ما يسمى سلطة الشهادات (Certification Authority)، اختصاراً CA لغرض التوثيق. يقوم CA أولاً بالتحقق من هوية الشخص A ثم يُكَوِّن رسالة تحتوي على المعلومات الشخصية (اسم، عنوان، وهكذا) إضافة إلى مفتاح A المعلن (α^a في حالتنا). يوقع CA الرسالة وبهذا يصدر شهادة C_A تربط هوية A مع

(٤) انظر التمرين (**١٢,٥,٥**) الذي يقترح برتوكولاً يجبر حواء على التصرف بحذر.

مفتاحها المعلن. يقوم أليس وبوب بتبادل الشهادتين C_A و C_B المتضمنتين α^a و α^b على التوالي. عند استلام بوب للشهادة C_A يتحقق من صواب توقيع CA ومن ثم يقتنع بأن مفتاح أليس المعلن هو α^a. وبالمثل، تقوم أليس بالتحقق من أن مفتاح بوب المعلن هو α^b. لا يزال احتمال انتحال الشخصية قائماً هنا؛ لأنه من الممكن أن ترسل حواء (العدو) شهادة تنتمي إلى أليس ومع ذلك فإنها غير قادرة على حساب المفتاح السري المشترك α^{ab}.

يحتاج استخدام CA بهذا الأسلوب إلى دفع ثمن (مرة واحدة) إنشاء شهادة لكل مستخدم ولكن التحقق من التواقيع لا يحتاج إلى تدخل من قبل CA. يجب أن يكون مفتاح CA المعلن موثقاً ولكن السرية غير مطلوبة هنا. أما نقاط الضعف هنا فتكمن في أن CA يخدم عدد كبير من العملاء وبالتالي يكون مستهدف من قبل العدو، وبالمقابل فإن إلغاء خدمات CA يؤدي إلى فاجعة. أيضاً، من الممكن أن يضطر CA إلى إلغاء المعلومات وإعادة التوزيع مرة أخرى في حالة انتهاء صلاحية شهادة العميل أو توقيع CA.

أحد الاستخدامات الشائعة للشهادات هو تأمين شراء منتجات آمن من خلال شبكة الاتصال العالمية (الإنترنت). في العادة يكون التوثيق باتجاه واحد (يرسل التاجر شهادة إلى العميل)؛ لأن إرسال شهادات من قبل العميل نادرة الحدوث. يكون لدى العميل الذي يستخدم برنامج الدخول إلى مواقع الشبكة العالمية قائمة بسلطات الشهادات حيث يقبل تواقيع هذه السلطات. من الممكن لهذا البرتوكول أن يسمح للعميل من التحقق من الشهادة. فالشهادة الصالحة من http://www.delta.com يكون لديها معلومات مقنعة بأن المفتاح المعلن هو بالفعل مفتاح www.delta.com. ومن الممكن أن تحدث مفاجئة للشخص الراغب في شراء تذكرة سفر لاكتشافه أن عنوان شركة دلتا للطيران هو www.delta-air.com [٥].

---

(٥) لاحظت detta Comm أن حوالي 8000 زائر في اليوم يدخلون إلى www.delta.com بغرض البحث عن Delta Air. وتم في العام ١٩٩٩م تعديل على صفحة الانترنت لتقليل الدخول غير المرغوب.

(١٢,٥,٢) براهين بدون معلومات

الهدف الذي تسعى أليس (المُبَرهِنة) إلى تحقيقه هو إقناع بوب (المتحقق) من أن بحوزتها سر s. أحد الخيارات لذلك هو أن تفصح أليس لبوب عن السر ومن ثم لا يبقى السر سراً. عند دراستنا لخطة توثيق كلمة السر التي ناقشناها في البند (**١٠,٣,٢**) حصل العدو على كلمة سر أليس ومن ثم أصبح باستطاعته انتحال شخصية أليس. يتيح برتوكول عدم المعرفة مطلقاً للمبرهن بتقديم إثبات مقنع أن بحوزته سراً دون إفشاء أي معلومات يستطيع المتحقق أن يستخدمها لاحقاً.

تحتاج المناقشة الدقيقة لبروتوكولات عدم المعرفة مطلقاً إلى معلومات ومفاهيم صعبة. ولذا ندعو القارئ المهتم لمثل هذه المناقشة الدقيقة اللجوء إلى المراجع المذكورة في البند (**١٢,٦**) حيث ذكرنا أيضاً مرجعين لمناقشة غير رياضية لمفهوم عدم المعرفة مطلقاً. سنقصر دراستنا في هذا البند على مناقشة غير دقيقة لهذا البرتوكول.

كتوضيح لأنظمة البراهين (ليست بالضرورة براهين عدم المعرفة مطلقاً) دعنا نناقش مسألة برهان أن $v \in J_n$ راسب غير تربيعي حيث n حاصل ضرب أعداد أولية كبيرة سرية. المبرهن الذي يعرف تحليل العدد n يستطيع تقديم برهان غير قابل للرفض بأن $v \in \overline{Q_n}$ وذلك بالكشف عن قواسم العدد ولكنه يكون قد قدم للمتحقق في هذه الحالة معلومات أكثر بكثير من اقناعه بأن v هو بالفعل راسب غير تربيعي.

قدم [40] البرهان التالي لهذه المسألة. لاحظ أن كلمة "برهان" في هذا السياق تعني "معلومات مقنعة" وليس معلومات مؤكدة.

(١) يقوم المتحقق B باختيار عدد $t > 0$ كوسيط لضمان الأمن ويختار أيضاً $b_i \in \{0,1\}$ عشوائياً. كما يختار $z_i \in \mathbb{Z}_n^*$ حيث $1 \le i \le t$. يتحدى B المبرهن A بالقيم:

$$w_i \equiv z_i^2 v^{b_i} \pmod n \quad ، \quad 1 \le i \le t.$$

(٢) يحدد A (بطريقة ما) إذا كان كل من w_i راسباً تربيعياً ويكون رده:

$$c_i = \begin{cases} 0 & , \quad w_i \in \overline{Q_n} \\ 1 & , \quad w_i \in Q_n \end{cases}$$

لكل $1 \leq i \leq t$.

(٣) يتحقق B ما إذا كان $b_i = c_i$ لكل i ، و إذا كان كذلك يقبل B البرهان (أن v راسب غير تربيعي).

إذا كان v راسباً غير تربيعي فإن التحدي w_i راسب تربيعي إذا وفقط إذا كان $b_i = 0$. فإذا كان t كبيراً كفاية وأن الفريقين التزما بالبرتوكول فسوف يقتنع B أن v راسب غير تربيعي. ومن ناحية أخرى، إذا كان v بالفعل راسباً تربيعياً فإن كلاً من w_i راسباً تربيعياً وأن احتمال أن يكون $b_i = c_i$ لكل i يساوي 2^{-t} وبهذا يكون من غير المرجح أن يقبل B بالادعاء $v \in \overline{Q_n}$.

إذا التزم الفريقان بالبرتوكول فلا يتاح للمتحقق B من معرفة أي معلومات لا يستطيع حسابها دون A (عدا حقيقة أن المبرهن قادر بالفعل على النجاح بالتحدي). هذا البرتوكول ليس عدم معرفة مطلقاً. كما أن المتحقق ليس مجبراً على الالتزام بالبرتوكول؛ لأنه من الممكن أن يحصل على رد لأعداد w_i من اختياره، أي أنه من الممكن أن يستخدم المتحقق المبرهن (بافتراض أن المبرهن لا يلجأ إلى الغش) لتحديد فيما إذا كانت أعداد من اختياره (ليس بالضرورة أن يكون على الصيغة الموصوفة بالبرتوكول) رواسب تربيعية. الصيغة المقدمة لهذا البرتوكول في [40] تفرض على المتحقق أن يكون أميناً.

كما ذكرنا سابقاً فإن أحد تطبيقات مفاهيم عدم المعرفة مطلقاً هي إثبات الهوية الشخصية. صمم البرتوكول التالي على البرهان بعدم المعرفة مطلقاً لإثبات أن قيمة معينة v هي راسب تربيعي قياس n.

برتوكول (إثبات الهوية الشخصية لفيات وشامير)

يختار مركز موثوق به قياس $n = pq$ مشابهًا لقياس RSA ويبقى القواسم سرية. يحصل المبرهن A على عدد سري $s \in \mathbb{Z}_n^*$ من المركز الموثوق به ويكون $v \equiv s^2 (\bmod n)$ مفتاح A المعلن. ينجح المبرهن في إقناع المتحقق B أن بحوزته s بتنفيذ الخطوات الثلاث التالية عدد t من المرات حيث $t > 0$ هو عدد لضمان الأمن :

(١) يختار A عشوائياً الالتزام (commitment) r حيث $1 \leq r < n$ ويرسل الشاهد $x \equiv r^2 (\bmod n)$ إلى B.

(٢) يرد B بتحدي عشوائي $e \in \{0,1\}$.

(٣) يكون رد A هو $y \equiv rs^e (\bmod n)$.

(٤) يتحقق B من أن $y \not\equiv 0$ وأن $y^2 \equiv xv^e (\bmod n)$. يقبل B البرهان إذا نجحت جميع الجولات وعددها t.

ليس لدى المتحقق B أي معلومات عن السر s : لا يعتمد الرد $y = r$ على s والعدد العشوائي r في الرد $y = rs$ غير معلوم من قبل B. من الممكن أن يتمكن العدو في كل جولة من انتحال شخصية A وينجح إذا كان التحدي متوقعاً. فإذا توقع أن يكون $e = 0$ فإن الشاهد والرد لا يتغيران، وإذا توقع أن يكون $e = 1$ فيقوم باختيار $x = r^2 v^{-1}$ كشاهد و $y = r$ كرد. وبما أن التحديات يتم اختيارها بطريقة عشوائية فإن احتمال نجاح التوقع يساوي $\frac{1}{2}$ في كل جولة. يبين التمرين (**١٢,٥,٢**) أنه على الأغلب يتم اكتشاف مثل هذا المتطفل. يمنع أيضاً عدم القدرة على توقع التحدي محاولة الكسر بإعادة لعب الجولات من قبل عدو بحوزته شهادة من جلسة برتوكول صحيحة سابقة.

(١٢,٥,٣) رمي النقود والبوكر الذهني

نقدم في هذا البند برتوكولان تعمويان إضافيان لغرض تسليط الضوء على التطبيقات الواسعة لمثل هذه البرتوكولات وكذلك للتأكيد على التحديد الواضح لفرضيات البرتوكول والتحقق من ملائمة هذه المتطلبات. يحتوي البند (**١٢,٦**) مراجع للعديد من التطبيقات الأخرى ومحاولات كسر مثل هذه البرتوكولات.

قدم بلم (Blum [11]) اقتراح رمي قطعة النقود باستخدام الهاتف. قرر الزوجان أليس وبوب بعد العديد من المشاحنات الانفصال عن بعضهما ومن ثم الطلاق واتفقا على استخدام الهاتف لرمي قطعة نقود ليحسما من سيكون له حق الوصاية على الأطفال. المعضلة هنا أن كليهما غير مستعد أن يكون المتصل الأول أو أن يفصح عن نتيجة رمي قطعة النقود. تكمن الفكرة الأساسية وراء هذا البرتوكول بأن أليس ستلتزم بالاختيار "صورة" أو "كتابة" وتعلن عن التزامها بطريقة تسمح لها بإخفاء اختيارها مع التزامها بهذا الاختيار. يقوم بوب بتخمين خيارها ومن ثم تقوم أليس بتقديم معلومات تجعل التزامها معلناً. يعتمد أمن البرتوكول على صعوبة حل مسألة الرواسب التربيعية (QRP).

برتوكول رمي قطعة نقود

(١) تختار أليس $n = pq$ حيث $p \neq q$ عددان أوليان فرديان وتختار عشوائياً $x \in J_n$ وتعلن عن n و x لبوب.

(٢) يكون رد بوب إما "$x \in Q_n$" أو "$x \in \overline{Q_n}$" (باحتمال 50% أن يكون صائباً بفرض صعوبة مسألة QRP).

(٣) تقوم أليس بالإفصاح عن p و q. يقوم بوب بالتحقق من أن p و q هما أوليان بالفعل (ومن ثم $x \in J_n$). يتحدد صواب رد بوب بحساب $\left(\dfrac{x}{p}\right)$.

إذا فشل بوب بالتحقق من أولية العددين p و q فيكون بإمكان أليس الغش بأخذ $n = p_1p_2p_3$ حيث p_i أعداد أولية واختيار x يحقق $\left(\frac{x}{p_1}\right) = \left(\frac{x}{p_2}\right) = -1$ و $\left(\frac{x}{p_3}\right) = 1$ (أي أن $\left(\left(\frac{x}{n}\right) = 1\right)$) وبعد حصول أليس على رد (تخمين) بوب تقوم بالإفصاح عن الزوج $(p = p_1, q = p_2p_3)$ أو الزوج $(p = p_1p_2, q = p_3)$ وذلك يعتمد على النتيجة التي تفضلها (على سبيل المثال، إذا أرادت أن يعتقد بوب أن x راسب تربيعي فإنها نفصح عن الزوج الأول).

لعبة البوكر ذهنياً

يظهر أن علماء التعمية لهم اهتمامٌ خاصٌ في لعبة عادلة (غير متحيزة) للبوكر الذهني. اقترح كل من شامير ورايفست وأدلمان في العام ١٩٧٩م برتوكولاً للتوزيع نشر العام ١٩٨١م في المجلة العلمية (The Mathematical Gardner). الفكرة الأساسية هي استخدام برتوكول الثلاث خطوات لشامير. اتفق أليس وبوب على مجموعة رسائل m_i ، $1 \le m_i \le 52$ رسالة لكل ورقة لعب. تقوم أليس بتعمية هذه الرسائل وترسل $E_{k_A}(m_i)$ ، $1 \le i \le 52$ بترتيب عشوائي. يختار بوب خمسة نصوص معماة ويعتبرها أوراق لعب أليس ويعيدها إلى أليس. يقوم بعد ذلك بتعمية خمسة نصوص معماة إضافية باستخدام E_{k_B} ويرسلها إلى أليس التي تستخدم D_{k_A} لإزالة قفلها عن هذه الرسائل وتعيد النتيجة إلى بوب على اعتبار أنها أوراق لعب بوب.

اقترح لهذه اللعبة توليد مفتاح شبيه لنظام RSA حيث يتفق أليس وبوب على عدد قياس n (حاصل ضرب عددان أوليان فرديان مختلفان) وكل منهما يختار مفتاح سري $k = (e, d)$ بحيث يكون $(e, \varphi(n)) = 1$ و $ed \equiv 1(\bmod \varphi(n))$. وبهذا تكون دالتي التعمية وكشف المعمى هما $E_k(m) \equiv m^e(\bmod n)$ و $D_k(c) \equiv c^d(\bmod n)$ على التوالي. يعلنان عن مفتاحيهما السريين بعد انتهاء اللعبة.

بعد نشر هذه الخطة بزمن قصير بين ليبتون (Lipton [25]) أن الدالة المقترحة تفشل ولا تحقق الفرضية الضمنية للبرتوكول التي تدعى عدم إمكانية تعليم أوراق اللعب ؛ وذلك لوجود خوارزمية فعالة لحساب رمز جاكوبي والمحافظة على القيمة بعد التعمية. أي أن :

$$\left(\frac{m}{n}\right) = \left(\frac{m}{n}\right)^e = \left(\frac{m^e}{n}\right)$$

فإذا لم تكن قيم رمز جاكوبي متساوية لكل m_i يكون بإمكان بوب اختيار أوراق لعب بقيم معينة لرمز جاكوبي ويعيدها إلى أليس وبهذا يحتمل حصوله على أفضلية. من الممكن هزيمة مثل هذا الهجوم باختيار تعمية لتكون جميعها رواسب تربيعية. يجد لاعب البوكر المهتم مراجع في البند (١٢,٦) لبرتوكولات مقترحة وطرق للغش.

تمارين

(١٢,٥,١) في برتوكول الثلاث خطوات لشامير افرض أن $E_k(m) \equiv m^k (\bmod p)$ حيث p عدد أولي مناسب.

(أ) أثبت أن دالة التعمية إبدالية وبهذا تحقق الشرط لاستخدام البرتوكول.

(ب) كيف يتم اختيار k_A و k_B؟ جد c_1 ، c_2 ، c_3.

(ج) ناقش أمن البرتوكول.

(١٢,٥,٢) يتعلق هذا التمرين ببرتوكول فيات وشامير لإثبات الهوية الشخصية.

(أ) إذا نجح منتحل الشخصية بتوقع التحدي e فأثبت أن الشاهد x والرد y سيقبلان بخطوة التحقق.

(ب) إذا كان التوقع خاطئاً فوضح كيفية اكتشاف منتحل الشخصية.

(**١٢,٥,٣**) (إثبات حوزة لوغاريتم منفصل (انظر [19,20])) افرض أن p عدد أولي وأن رتبة $g \in \mathbb{Z}_p^*$ هو العدد الأولي q. المفتاح السري للمستخدم A هو s حيث $1 \leq s < q$ والمفتاح المعلن هو $S \equiv g^s (\mathrm{mod}\, p)$. يقنع A المستخدم B بحوزته s في عدد $t > 0$ من الجولات.

(١) يختار A عشوائياً التزام x ، $1 \leq x < q$ ويرسل الشاهد $X \equiv g^x (\mathrm{mod}\, p)$ إلى B.

(٢) يرد B بتحدي عشوائي $e \in \{0,1\}$.

(٣) يكون رد A على النحو التالي

$$y = \begin{cases} x & ,e = 0 \\ sx^{-1} (\mathrm{mod}\, q) & , \quad e = 1 \end{cases}.$$

يقبل B البرهان إذا تم نجاح جميع الدورات التي عددها t.

(أ) إذا التزم الفريقان بقواعد البرتوكول فتحقق من أن B سيقبل البرهان.

(ب) بين كيف يتمكن المتطفل من الغش بافتراض إمكانية تخمين التحديات (ولكن s غير معلوم).

(ج) ناقش المعضلة التي ستواجه العدو في حالة التخمين الخاطئ.

(**١٢,٥,٤**) خطة مقترحة لإثبات الهوية الشخصية. تقوم سلطة الشهادات بربط هوية أليس بالعدد $n = pq$ حيث n معلن والعددان الأوليان $p \neq q$ هما مفتاح أليس السري.

(١) يتحدى بوب أليس براسب تربيعي عشوائي x قياس n.

(٢) يكون رد أليس جذر تربيعي y للعدد x.

(٣) يتحقق بوب من صواب $y^2 \equiv x (\mathrm{mod}\, n)$.

إذا نجحت الخطوات بعدد من الجولات فهل هذا كافياً لإقناع بوب بحوزة أليس على سر؟ بين أن هذه الخطة تحتوي على عيوب مقلقة.

(**١٢,٥,٥**) (تبادل مفاتيح بوجود أعداء نشطين) لنفرض أن أليس وبوب يعتمدان على تمييز الأصوات أثناء جلسة تبادل المفاتيح. ولهذا عوضاً عن استخدام سر ديفي وهيلمان المشترك α^{ab} مباشرة فإنهما يستخدمان وسيلة تمييز الأصوات وكل منهما سيقرأ جزءاً من السر α^{ab}. بعد التحقق من هذه الأجزاء للسر α^{ab} يكون الجزء المتبقي هو السر المشترك k.

(أ) بافتراض أن العدو غير قادر على معرفة k من α^{a} و α^{b} والأجزاء التي تم تسريبها من α^{ab}. هل هذا مقنع لكل من أليس وبوب بأن العدو لا يعرف k ؟

اقترح رايفست وشامير [72] تغيير في هذا البرتوكول يجبر المعترض في المنتصف من إخفاء نشاطه (ومن ثم يحتمل الكشف عن وجوده). تختار أليس رسالة m وترسل نصف $E_k(m)$ حيث k هو المفتاح التي تم حسابه (من المحتمل أن يكون مشتركاً مع العدو وليس مع بوب). يقوم بوب بالرد بنصف النص المعمى الذي يختاره. بعد ذلك تقوم أليس بإرسال النصف الآخر من الرسالة $E_k(m)$ ويقوم بوب بالرد بصورة مماثلة.

(ب) افرض عدم امكانية اكتشاف بعض أجزاء النص الواضح من معرفة نصف $E_k(m)$ فقط. ناقش خيارات العدو (بالتحديد، ناقش ماذا يحصل إذا قام العدو بإرسال النصف الأول من رسالة أليس).

(**١٢,٥,٦**) (قناة مخفية Subliminal Channel) يمكن لخطط التوثيق أن تسمح بوجود قناة مخفية يتواصل بها فريقان دون التمكن من اكتشافها. اقترح سيمونز (simmons [82, 83]) التصور (السيناريو) التالي لمسألة يطلق عليها مسألة السجين:

> ارتكب مجرمان جريمة مشتركة وتم اعتقالهم وسجنهم في زنزانتين منفصلتين بعيدتين عن بعضهما لحين تقديمهما للمحاكمة. طريقة التواصل الوحيدة بينهما هي عن طريق

إرسال رسائل لبعضهما من خلال طرف ثالث موثوق من إدارة السجن (يفترض أن يكون عميل لمدير السجن). يسمح مدير السجن للسجينين بالتواصل على أمل أن يتمكن من خداع على الأقل واحداً منهما بأن يقوم بإرسال رسالة من إدارة السجن إلى أحد السجينين وإقناعه أن من كتبها هو زميله السجين الآخر أو على الأقل تعديل في رسالة حقيقية أرسلت من زميله. وبما أن لدى مدير السجن قناعة تامة بأن السجينين سيحاولان الاتفاق على خطة تؤدي إلى تملصهم من ذنب ارتكاب الجريمة فإن مدير السجن سيسمح لهم فقط بالتواصل على شرط قراءته لجميع رسائلهم وبأن تكون رسائلهم غير ضارة. ومن ناحية أخرى فالسجينين ليس لديهما أي خيار إلا قبول شروط مدير السجن. أي، أن يقبلان باحتمال خداعهما أفضل من عدم تواصلهما إطلاقاً؛ وذلك لأنهما بحاجة إلى الاتفاق على وضع خطة للتملص من الجريمة. ولكي ينجحا في ذلك فيجب أن يجدا وسيلة لخداع مدير السجن؛ وذلك بإيجاد خطة سرية للتواصل بينهما. أي إيجاد "قناة مخفية" بينهما على مرأى ومسمع مدير السجن على الرغم من أن الرسائل بينهما لا يظهر أنها تحتوي على معلومات سرية (على الأقل لمدير السجن). وبما أنهما على يقين من نية مدير السجن لخداعهما بزج رسائل مزورة فإنهما يوافقان على التواصل بشرط أن يسمح لهما بتوثيق رسائلهما.

يسمح توقيع الجمل بوجود مثل هذه القناة المخفية بين السجينين أليس وبوب. توليد مفتاح أليس لا يتغير حيث تقوم أليس باختيار عدد أولي p ومولّد $\alpha \in \mathbb{Z}_p^*$. وتختار عدداً عشوائياً سرياً a ، $1 \leq a \leq p-2$. وبهذا يكون مفتاح أليس المعلن هو $\left(p, \alpha, \alpha^a (\bmod p)\right)$. عادة، تقوم أليس بتوقيع الرسالة m باختيار عشوائي k حيث $k < p$ و $(k, p-1) = 1$ ومن ثم حساب (r, s) حيث $r \equiv \alpha^k (\bmod p)$ ونحصل على s بحل التطابق:

$$H(m) \equiv ar + ks (\bmod p-1)$$

عندئذ، تقوم بإرسال (m, r, s) إلى بوب عن طريق مدير السجن. أما إذا أرادت أليس مشاركة السر a مع بوب فمن الممكن استخدام k لنقل الرسالة المخفية[٦].

(أ) إذا اشترك كل من أليس وبوب في السر a، فما هي الشروط التي يجب أن يحققها s بحيث يكون باستطاعة بوب إيجاد القناة المخفية k بطريقة فعالة بمعرفة (m, r, s)؟

المعضلة التي تواجه أليس هي مشاركة مفتاحها السري مع بوب (مع احتمال أن يكون بوب قادراً على تزوير توقيعها). وعلى الرغم من ضرورة إرسال المفتاح a بطريقة آمنة إلا أن يونغ وينغ (Young and Yung) قدما SETUP (انظر التمرين (**١٢,٢,١٤**)) طريقة تسمح لأليس من الكشف عن مفتاحها السري لبوب باشتراط أن يكون مفتاح بوب المعلن $\left(p, \alpha, \alpha^b (\bmod p)\right)$ معروفاً لأليس. عندئذ، تقوم أليس بتلويث خطوات التوقيع وينتج عن ذلك (m_1, r_1, s_1) و (m_2, r_2, s_2) بطريقة تسمح للمستخدم الذي لديه b من معرفة a. ولكي تكشف أليس عن a تختار عشوائياً k_1 بحيث يكون كل من k_1 و $\beta \equiv \left(\alpha^b\right)^{k_1} (\bmod p)$ و $\alpha^{\beta^{-1}} (\bmod p)$ أولية نسبياً مع $p - 1$ حيث β^{-1} هو النظير الضربي للعدد β قياس $p - 1$. وعوضاً

---

(٦) على الرغم من أن توقيع الجمل (r, s) يحتاج إلى $2 \log_2 p$ مرتبة ثنائية إلا أن $\log_2 p$ مرتبة ثنائية فقط تستخدم للسرية ومن ثم فباقي المراتب يمكن استخدامها للقناة المخفية. وبما أن $(k, p-1) = 1$ فمن الممكن إرسال فقط $\varphi(p-1)$ من الرسائل السرية المختلفة k ويكون من الصعب اكتشافها لأن للتطابق $xs \equiv H(m) - ar (\bmod p - 1)$ العديد من الحلول x. لاحظ سيمونز [84, 85] إمكانية التغلب على نقاط الضعف هذه عند استخدام DSA والمفترض أن هذا النظام هو الأفضل بسماح وجود قنوات مخفية لحد الآن.

عن اختيار أليس للعدد k_2 عشوائياً فإنها تختار $k_2 = \beta^{-1}$. أخيراً، افرض كالعادة أن $r_i \equiv \alpha^{k_i} (\bmod\, p)$ و $s_i \equiv (H(m_i) - ar_i)k_i^{-1} (\bmod\, p-1)$، حيث $i \in \{1,2\}$.

(ب) أثبت أن باستطاعة بوب الحصول على a بحساب $r_2^{-1}\left(H(m_2) - s_2 \,/\, r_1^b (\bmod\, p)\right)(\bmod\, p-1)$.

(ج) لغرض التوضيح، افرض أن $p = 13$ ، $\alpha = 2$. أثبت أن كلاً من β و $\alpha^{\beta^{-1}} (\bmod\, p)$ أولي نسبياً مع $p-1$ إذا كان $b = 5$ و $k_1 = 7$. إذا كان $b = 3$ فأثبت عدم قدرة أليس على إيجاد k_1 يحقق الخواص المطلوبة.

(١٢,٦) حواشي
Notes

إضافة إلى خطط التعمية التي درسناها في هذا الكتاب، توجد طرق تعمية أخرى ذات أهمية خاصية تعتمد على المنحنيات الناقصية. حيث تضمن هذه الطرائق أمن النظام بمفتاح أقصر مقارنة مع الأنظمة الأخرى كنظام RSA. فخوارزمية المنحنيات الناقصية للتوقيع الالكتروني (Elliptic Curve Digital Signature Algorithm) أو اختصاراً ECDSA هي رديف DSA وتم قبولها من قبل معهد القياس الوطني الأمريكي (American National Standards Institnte) أو اختصاراً (ANSI X9.62) في العام ١٩٩٩م. تجد في مرجع جونسن ومينيزس (Johnson and Menezes [44]) دراسة تتعلق بقرارات التصميم و الأمن و التنفيذ للتوقيع ECDSA كما يتضمن بحثهما مقدمة عن المنحنيات الناقصية. أما كوبلتز (Koblitz [50]) وستنسون (Stinson [86]) فيحتويان على مقدمة للمنحنيات الناقصية وتطبيقاتها في التعمية. وأما المواضيع المتقدمة في المنحنيات الناقصية فمن الممكن إيجادها في العديد من المراجع نذكر منها بلاك وسيروسي وسمارت (Blake, Seroussi, and Smart [8]) ومينيزس (Menezes [62]).

ذكر التقرير التقني الذي أعلن عنه في العام ١٩٩٧م من قبل مجموعة الأمن للاتصالات الإلكترونية، اختصاراً (CESG) أن علماء التعمية البريطانيون استخدموا أنظمة التعمية ذوات المفاتيح المعلنة في العام ١٩٧٠م حيث أطلقت عليه مجموعة CESG [30] العنوان "تعمية غير سرية" وظهر نظام تعمية شبيه بنظام RSA في المرجع كوكس (Cocks [21]). كما أن فكرة خطة ديفي وهيلمان لتبادل المفاتيح ظهرت في وليمسن (Williamson [100])(٧).

هناك عديد من التطبيقات المشهورة التي تستخدم أنظمة التعمية التقليدية وأنظمة التعمية ذوات المفاتيح المعلنة معاً للحصول على توثيق وسرية، ومن هذه التطبيقات "سرية جيدة جداً" (PGP)، انظر [37,104] وعلى صعيد الأنظمة، نظام ميكروسن المعروف باسم آلية إنجاز الاتصال البعيد (remote procedure call) أو اختصاراً RPC، انظر [70,88]. من المهم ذكره هنا أن جزءاً من أمن خطة ميكروسن تعتمد على أخذ القوة قياس عدد أولي طوله 192 مرتبة ثنائية والذي اعتبر غير آمن في العام ١٩٩١م [54]. ولاعتبارات عدم التعرض للهجوم يجب الأخذ بالاعتبار الإطار العام لأمن الشبكة و التي لا تعتمد فقط على مبادئ تعموية. في واقع الأمر، إن مسائل الأمن لا تعتمد في الغالب على التعمية. شهد العام ١٩٩٠م سيل من الإنذارات الأمنية

---

(٧) علقت مجموعة CESG بالقول "من المهم ذكره أنه على الرغم من اقتراح العديد من الأفكار لأنظمة التعمية ذوات المفاتيح المعلنة، إلا أن أفضل نظامين آمنين هما أول نظامين تم اكتشافهما. كما أنه من المهم ملاحظة أن ترتيب الأكاديميين لهذه الاكتشافات هو عكس ترتيب مجموعة CESG". كتب وليمسون [100] كلمات حذرة في مقدمة كتابه: "أحد الأسباب التي جعلتني أرجئ الكتابة هو أنني أجد نفسي في وضع محرج، وبعد كتابة الكتاب [99] بدأت أشك في مجمل نظرية التعمية غير السرية. والمشكلة تتلخص في أنني لا أملك برهاناً أن الطريقة المقدمة في [99] هي بالفعل آمنة. وبصيغة أخرى، فيما إذا كان لهذه الطريقة ضمانات لعدم كسرها".

بسبب بعض التجاوزات مثل الرسائل التي طولها يزيد عن الطول المفترض واحتواء بعض الرسائل على رموز غير متوقعة. وكانت بعض هذه التجاوزات في البرامج المعنية بآلية الأمن.

أخذت المواضيع التي تتعلق بالبراهين بدون معلومات من جولدواسر وميكالي وراكوف ([40] Golodwasser, Micali, and Rackoff) ومن مينيزس وفان أورشت وفانستون ([63] Menezes, Van Oorshot, and Vanstone). انظر أيضاً الفصل الثالث عشر من كتاب ستنسون [86]. صنف براسارد و سربيو ([18] Brassard and Cre'peau) المفاهيم المتعددة لبراهين بدون معلومات.

وما يثير الاهتمام (أو على الأقل التعجب) هو جلسات CRYPTO التي ناقشت مقدمة لبرهان بدون معلومات دون استخدام الرياضيات حيث قدم كوسيكواتر وجوليو وبرسون ([68] Quisquater, Guillou, and Berson) مقالة بعنوان "مغارة علي بابا الغريبة" التي يؤدي مدخلها إلى تشعبات من الطرق غير النافذة. وصمم اختبار عملي يبين قدرة المدعي على تقديم برهان مقنع من امتلاكه كلمات سحرية تمكنه من فتح ممراً بين النهايات غير النافذة دون الإفصاح عن السر نفسه. طلب من المدعي الذي دخل المغارة بمفرده سابقاً من العودة باستخدام طريق من اختيار شاهداً يقف عند التشعب. تكرر إعادة التجربة لغاية اقتناع الشاهد بأن المدعي يمتلك فعلاً كلمات سحرية(٨).

في العام ١٩٩٨م قدم مفهوم البرهان بدون معلومات في أحد لقاءات CRYPTO على شكل لعبة بعنوان أين والدو ([41] Where's Waldo) والهدف من هذه اللعبة هو تحديد مكان الشخصية والدو. في هذه اللعبة يكون المطلوب من أليس إقناع بوب بأنها

---

(٨) كان من الممكن تقديم البرهان لخطوة واحدة وذلك بسؤال المدعي بعمل دورة مبتدأ من التشعب، أو على الأصح إتلاف القصة.

وجدت والدو دون الإفصاح عن الحل (كيفية إيجاده). ستستخدم مقصاً خاصاً بها لإخفاء والدو من الخلفية ولكن هذا لا يقنع بوب حيث يتهمها باستخدام صورة أخرى من مصدر آخر. يكون حل أليس هو استخدام قطعة ورق معتمة حجمها ضعف حجم صورة والدو و تحتوي على نافذة صغيرة لعزل والدو.

تحتوي المراجع سالوما (Salomaa [75]) وسيبري وبيرايك (Seberry and Pieprzyk [77]) وشناير (Schneier [76]) على عديد من مجالات تطبيقات البرتوكولات مثل، مشاركة السر، القنوات المخفية، النقود الإلكترونية، خطط الاقتراع وغيرها. وقدم سيمونز (Simmons [84]) عرض شامل للقنوات المخفية حيث استهل هذا العرض بمقدمة تاريخية تتعلق بالتحقق من العرض المقدم لاتفاقية الحد من الأسلحة الإستراتيجية المعروفة باسم SALTII. يستطيع القارئ إيجاد بروتوكولات تقترح طرق الغش في لعبة البوكر الذهنية في فورتشن وميريت (Fortune and Merritt [33]) وكوبرسميت (Coppersmith [22]) وغيرها.

الملاحق

الملحق (أ): خوارزمية إقليدس

الملحق (ب): تحليل $x^n + 1$

الملحق (ج): مثال على تشفير قرص مدمج

الملحق (د): حلول لتمارين مختارة

الملحق (أ)

خوارزمية إقليدس
The Euclidean Algorithm

القاسم المشترك الأكبر (اختصاراً gcd) لكثيرتي حدود $f(x), g(x) \epsilon K[x]$ هو كثيرة الحدود $d(x) \in K[x]$ التي درجتها أكبر ما يمكن وتحقق $f(x) = q_1(x)d(x)$ و $g(x) = q_2(x)d(x)$ ونكتب عادة $\gcd(f(x), g(x)) = d(x)$.

مثال (١,١)

لنفرض أن:

$f(x) = 1 + x^2 + x^3 + x^6 + x^7 + x^8$ و $g(x) = 1 + x^3 + x^5 + x^6$.

بتحليل كل من $f(x)$ و $g(x)$ كحاصل ضرب كثيرات حدود غير قابلة للتحليل نرى أن:

$$f(x) = (1 + x)(1 + x + x^3)(1 + x^4)$$
$$g(x) = (1 + x)(1 + x^2)(1 + x + x^3)$$

كثيرة الحدود ذات الدرجة الأعلى بحيث تقسم كلاً من $f(x)$ و $g(x)$ هي $1 + x + x^3$. إذن،

$$\gcd(f(x), g(x)) = 1 + x + x^3 \qquad \blacktriangle$$

إن تحليل $f(x)$ و $g(x)$ إلى عوامل غير قابلة للتحليل لإيجاد القاسم المشترك الأكبر ليس بالطريقة الفعّالة. ولكن الخوارزمية التالية تقدم لنا طريقة فعّالة لإيجاد القاسم المشترك الأعظم لكثيرتي حدود.

خوارزمية إقليدس

لتكن $f(x), g(x) \epsilon K[x]$ حيث $\deg(f(x)) \geq \deg(g(x))$ و $g(x) \neq 0$.

(١) ضع $r_0(x) = f(x)$ ، $r_1(x) = g(x)$ ، $i = 1$.

(٢) إذا كان $r_i(x) > 0$ نقوم بقسمة $r_i(x)$ على $r_{i-1}(x)$ ونفرض أن $r_{i+1}(x)$ هو باقي القسمة. أي أن $r_{i+1}(x) \equiv r_{i-1}(x)(mod\, r_i(x))$.

(٣) إذا كان $r_{i+1}(x) > 0$ نكرّر الخطوة **(٢)**.

(٤) إذا كان $r_i(x) = 0$ نتوقف ويكون $\gcd(f(x), g(x)) = r_{i-1}(x)$.

لاحظ أن هذه الخوارزمية يجب أن تتوقف بعد عدد منته من الخطوات؛ لأنه لكل $i > 1$ تكون درجة الباقي $r_{i+1}(x)$ أصغر من درجة الباقي $r_i(x)$.

من الممكن تحسين هذه الخوارزمية للحصول على $t_i(x), s_i(x) \epsilon K[x]$ تحققان $t_i(x) f(x) + s_i(x) g(x) = r_i(x)$ لكل $i = 0,1,2,\cdots$ على النحو التالي:

بوضع:

$$t_0(x) = 1 \quad t_1(x) = 0$$
$$s_0(x) = 0 \quad s_1(x) = 1$$

وبفرض أن $r_{i-1}(x) = q_i(x) r_i(x) + r_{i+1}(x)$ (باستخدام خوارزمية القسمة) ووضع:

$$t_i(x) = q_{i-1}(x) t_{i-1}(x) + t_{i-2}(x)$$
$$s_i(x) = q_{i-1}(x) s_{i-1}(x) + s_{i-2}(x)$$

لكل $i = 2,3,\cdots$ نجد أن :

$$r_j(x) = (-1)^j[-t_j(x)r_0(x) + s_j(x)r_i(x)]$$
$$= t_j(x)r_0(x) + s_j(x)r_1(x)$$

وبما أن الحقل هو حقل ثنائي فنستطيع تجاهل الاشارة السالبة.

مثال (١,٢)

سنستخدم خوارزمية القسمة لإيجاد القاسم المشترك الأكبر لكثيرتي الحدود :

$$f(x) = x^2 + x^3 + x^6 + x^7$$
$$g(x) = 1 + x^3 + x^4 + x^5$$

ضع $i = 0$ ، $r_0(x) = f(x)$ ، $r_1(x) = g(x)$. بقسمة $r_0(x)$ على $r_1(x)$ نحصل على :

$$x^2 + x^3 + x^6 + x^7 = (1 + x^3 + x^4 + x^5)(1 + x^2) + (1 + x^4)$$

إذن ، $r_2(x) = 1 + x^4$ و $q_1(x) = 1 + x^2$. بقسمة $r_1(x)$ على $r_2(x)$ نحصل على :

$$1 + x^3 + x^4 + x^5 = (1 + x^4)(1 + x) + (x + x^3).$$

إذن ، $r_3(x) = x + x^3$ و $q_2(x) = 1 + x$. بقسمة $r_2(x)$ على $r_3(x)$ نحصل على :

$$1 + x^4 = (x + x^3)(x) + (1 + x^2).$$

إذن ، $r_4(x) = 1 + x^2$ و $q_3(x) = x$. بقسمة $r_3(x)$ على $r_4(x)$ نحصل على :

$$x + x^3 = (1 + x^2)(x) + 0.$$

إذن ، $r_5(x) = 0$ ويكون $\gcd(f(x), g(x)) = r_4(x) = 1 + x^2$.

إذا أردنا استخدام خوارج القسمة $q_i\left(x\right)$ لحساب $t_i\left(x\right)$ و $s_i\left(x\right)$ لكل من الخطوات $i = 0,1,2,3,4$ بحيث يكون:

$$r_i\left(x\right) = t_i\left(x\right) f\left(x\right) + s_i\left(x\right) g(x).$$

فنرى أن:

$$\begin{aligned} r_2\left(x\right) &= r_0\left(x\right) + q_1\left(x\right) r_1(x) \\ &= \left(1\right) f\left(x\right) + \left(1 + x^2\right) g(x) \end{aligned}$$

$$\begin{aligned} r_3\left(x\right) &= x + x^3 \\ &= \left(1 + x\right) f\left(x\right) + \left(x + x^2 + x^3\right) g(x) \end{aligned}$$

$$\begin{aligned} r_4\left(x\right) &= 1 + x^2 \\ &= \left(1 + x + x^2\right) f\left(x\right) + \left(x + x^3 + x^4\right) g(x) \end{aligned}$$

والجدول التالي يلخص لنا هذه الخطوات:

i	$t_i(x)$	$s_i(x)$	$r_i(x)$
0	1	0	$f(x)$
1	0	1	$g(x)$
2	1	$1 + x^2$	$1 + x^4$
3	$1 + x$	$x + x^2 + x^3$	$x + x^3$
4	$1 + x + x^2$	$1 + x^3 + x^4$	$1 + x^2$
	—	—	0

باستخدام الاستقراء الرياضي نحصل على المبرهنة التالية:

مبرهنة (١,٣)

إذا كان $\gcd(f\left(x\right), g\left(x\right)) = d(x)$ فيوجد $t\left(x\right), s(x) \epsilon K[x]$ بحيث يكون:

$$t\left(x\right) f\left(x\right) + s\left(x\right) g\left(x\right) = d(x).$$

تمارين

(١,٤) جد القاسم المشترك الأكبر لكل زوج من أزواج كثيرات الحدود التالية :

(أ) $g\left(x\right) = 1 + x + x^3 + x^5$, $f\left(x\right) = 1 + x + x^5 + x^6 + x^7$.

(ب) $g\left(x\right) = 1 + x + x^3$, $f\left(x\right) = 1 + x^2 + x^3 + x^7$.

(ج) $g\left(x\right) = 1 + x^2 + x^3 + x^7$, $f\left(x\right) = 1 + x + x^4 + x^5 + x^8 + x^9$.

(د) $g\left(x\right) = x + x^3 + x^4$, $f\left(x\right) = 1 + x + x^2 + x^3 + x^4$.

(١,٥) جد $\gcd(f\left(x\right), g\left(x\right))$ حيث $f\left(x\right) = 1 + x^9$ و $g(x)$ هي :

(أ) $g\left(x\right) = x + x^2 + x^4 + x^5 + x^7 + x^8$.

(ب) $g\left(x\right) = x^3 + x^6$.

(ج) $g\left(x\right) = 1 + x + x^2 + x^4 + x^5 + x^7 + x^8$.

(د) $g\left(x\right) = 1 + x^3 + x^6$.

(هـ) $g\left(x\right) = x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8$.

(١,٦) جد $\gcd(f\left(x\right), g\left(x\right))$ حيث :

$f\left(x\right) = 1 + x^{15}$ و $g\left(x\right) = x + x^2 + x^4 + x^8$.

(١,٧) جد $\gcd(f\left(x\right), g\left(x\right))$ حيث $f\left(x\right) = 1 + x^{23}$ و

$g\left(x\right) = x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}$.

الملحق (ب)

تحليل $1 + x^n$

Factorization of $1 + x^n$

الجدول التالي يُبيّن لنا تحليل $1 + x^n$ إلى حاصل ضرب كثيرات حدود غير قابلة للتحليل لكل عدد فردي n حيث $1 \leq n \leq 31$.

n	التحليل
1	$1+x$
3	$\left(1+x\right)\left(1+x+x^2\right)$
5	$\left(1+x\right)\left(1+x++x^2+x^3+x^4\right)$
7	$\left(1+x\right)\left(1+x+x^3\right)\left(1+x^2+x^3\right)$
9	$\left(1+x\right)\left(1+x+x^2\right)\left(1+x^3+x^6\right)$
11	$\left(1+x\right)(1+x+\cdots+x^{10})$
13	$\left(1+x\right)(1+x+\cdots+x^{12})$
15	$\left(1+x\right)\left(1+x+x^2\right)\left(1+x+x^2+x^3+x^4\right)\left(1+x+x^4\right)\left(1+x^3+x^4\right)$
17	$\left(1+x\right)\left(1+x+x^2+x^4+x^6+x^7+x^8\right)\left(1+x^3+x^4+x^5+x^8\right)$
19	$\left(1+x\right)(1+x+x^2+\cdots+x^{18})$
21	$\left(1+x\right)\left(1+x+x^2\right)\left(1+x^2+x^3\right)\left(1+x+x^3\right)$
	$\left(1+x^2+x^4+x^5+x^6\right)\left(1+x+x^2+x^4+x^6\right)$

n	التحليل
23	$(1+x)(1+x+x^5+x^6+x^7+x^9+x^{11})$
	$(1+x^2+x^4+x^5+x^6+x^{10}+x^{11})$
25	$(1+x)(1+x+x^2+x^3+x^4)(1+x^5+x^{10}+x^{15}+x^{20})$
27	$(1+x)(1+x+x^2)(1+x^3+x^6)(1+x^9+x^{18})$
29	$(1+x)(1+x+\cdots+x^{28})$
31	$(1+x)(1+x^2+x^5)(1+x^3+x^5)(1+x+x^2+x^3+x^5)$
	$(1+x+x^2+x^4+x^5)(1+x+x^3+x^4+x^5)(1+x^2+x^3+x^4+x^5)$

الملحق (ج)

مثال على تشفير قرص مدمج
Example of Compact Disc Encoding

يحتاج تقديم مثال لتشفير قرص مدمج إلى كمية كبيرة من الحسابات (انظر البند (٧،٣))، ولذا فسنقدم هنا مثالاً معقولاً بحيث يمكن إجراء الحسابات دون الحاجة إلى وسائل الكترونية. لتكن C شفرة ريد وسولومن على الحقل $GF(2^4)$ بمولّد:

$$g(x) = (1+x)(\beta+x)(\beta^2+x)(\beta^3+x)$$
$$= \beta^6 + \beta^0 x + \beta^4 x^2 + \beta^{12} x^3 + x^4$$

هذه شفرة من النوع $(15,11,5)$ والتي يمكن قصرها إلى شفرة C_1 من النوع $(8,4,5)$ أو شفرة C_2 من النوع $(12,8,5)$. ويمكن توريقها بعمودين لعمق 8. يمكن تشفير رسالة m إلى كلمة شفرة c في الشفرة C_1 باستخدام مصفوفة مولّدة (انظر الجدول (١،٣)).

الجدول (٣,١). رسالة والتشفير الأول.

	β^4	0	0	β^3		β^{10}	β^4	β^8	β^3	β^7	β^7	β^0	β^3
	β^1	β^{12}	β^3	0		β^7	β^9	β^4	β^{10}	β^4	β^{11}	β^3	0
	0	0	β^2	β^4		0	0	β^8	β^4	β^{12}	β^6	β^5	β^4
	0	0	0	β^{13}		0	0	0	β^4	β^{13}	β^2	β^{10}	β^{13}
	β^1	0	0	0		β^7	β^1	β^5	β^{13}	β^1	0	0	0
	0	β^3	β^2	0		0	β^9	β^{13}	β^{12}	β^{13}	β^0	β^2	0
	0	0	0	0		0	0	0	0	0	0	0	0
$m =$	β^4	β^4	0	β^1	$\to c =$	β^{10}	β^2	β^5	β^6	β^4	β^8	β^{13}	β^1
	0	0	0	0		0	0	0	0	0	0	0	0
	0	0	0	0		0	0	0	0	0	0	0	0
	β^1	0	0	0		β^7	β^1	β^5	β^{13}	β^1	0	0	0
	0	0	0	0		0	0	0	β^6	β^0	β^4	β^{12}	β^0
	0	0	0	0		0	0	0	0	0	0	0	0
	0	0	0	0		0	0	0	0	0	0	0	0
	0	0	0	0		0	0	0	0	0	0	0	$0\cdots$

تظهر هذه الكلمات في الشفرة C_1 للتوريق البيني على النحو التالي:

$$
\begin{array}{ccccccccccccccccccc}
\beta^{10} & \beta^7 & 0 & 0 & \beta^7 & 0 & 0 & \beta^{10} & 0 & 0 & \beta^7 & 0 & 0 & 0 & 0 & \cdots & & & \\
 & & \beta^4 & \beta^9 & 0 & 0 & \beta^1 & \beta^9 & 0 & \beta^2 & 0 & 0 & \beta^1 & 0 & 0 & 0 & 0 & \cdots & \\
 & & & & \beta^8 & \beta^4 & \beta^8 & 0 & \beta^5 & \beta^{13} & 0 & \beta^5 & 0 & 0 & \beta^5 & 0 & 0 & 0 & 0 \\
 & & & & & & \beta^3 & \beta^{10} & \beta^4 & \beta^4 & \beta^{13} & \beta^{12} & 0 & \beta^6 & 0 & 0 & \beta^{13} & \beta^6 & 0 \\
 & & & & & & & & \beta^7 & \beta^4 & \beta^{12} & \beta^{13} & \beta^1 & \beta^{13} & 0 & \beta^4 & 0 & 0 & \beta^1 \\
 & & & & & & & & & & \beta^7 & \beta^{11} & \beta^6 & \beta^2 & 0 & \beta^0 & 0 & \beta^8 & 0 \\
 & & & & & & & & & & & & \beta^0 & \beta^3 & \beta^5 & \beta^{10} & 0 & \beta^2 & 0 \\
 & & & & & & & & & & & & & & \beta^3 & 0 & \beta^4 & \beta^{13} & 0
\end{array}
$$

يمكن اعتبار أعمدة الصفيف أعلاه على أنها رسائل ونقوم بتشفيرها إلى كلمات في الشفرة C_2 حيث كل من صفوف الجدول التالي هو كلمة شفرة:

$$
\begin{array}{cccccccccccc}
\beta^{1} & \beta^{10} & \beta^{14} & \beta^{7} & \beta^{10} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
\beta^{13} & \beta^{7} & \beta^{11} & \beta^{4} & \beta^{7} & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \beta^{10} & \beta^{4} & \beta^{8} & \beta^{1} & \beta^{4} & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \beta^{0} & \beta^{9} & \beta^{13} & \beta^{6} & \beta^{9} & 0 & 0 & 0 & 0 & 0 & 0 \\
\beta^{13} & \beta^{7} & \beta^{10} & \beta^{5} & \beta^{2} & \beta^{5} & \beta^{8} & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \beta^{10} & \beta^{4} & \beta^{8} & \beta^{1} & \beta^{4} & 0 & 0 & 0 & 0 & 0 \\
0 & \beta^{7} & \beta^{7} & \beta^{14} & \beta^{9} & \beta^{12} & \beta^{2} & \beta^{3} & 0 & 0 & 0 & 0 \\
\beta^{1} & \beta^{5} & \beta^{4} & \beta^{2} & \beta^{6} & \beta^{4} & \beta^{7} & \beta^{10} & 0 & 0 & 0 & 0 \\
0 & 0 & \beta^{11} & \beta^{0} & \beta^{2} & \beta^{9} & \beta^{9} & 0 & \beta^{7} & 0 & 0 & 0 \\
0 & \beta^{8} & \beta^{10} & \beta^{5} & \beta^{14} & \beta^{8} & \beta^{9} & \beta^{0} & \beta^{4} & 0 & 0 & 0 \\
\beta^{13} & \beta^{7} & \beta^{11} & 0 & \beta^{11} & \beta^{5} & \beta^{11} & \beta^{14} & \beta^{6} & \beta^{7} & 0 & 0 \\
0 & 0 & \beta^{11} & \beta^{11} & \beta^{5} & \beta^{11} & \beta^{5} & \beta^{14} & \beta^{3} & \beta^{11} & 0 & 0 \\
0 & \beta^{7} & \beta^{1} & \beta^{5} & \beta^{5} & \beta^{12} & \beta^{5} & \beta^{7} & \beta^{14} & \beta^{4} & \beta^{0} & 0 \\
0 & 0 & 0 & \beta^{12} & \beta^{12} & \beta^{12} & \beta^{1} & \beta^{12} & \beta^{12} & \beta^{8} & \beta^{3} & 0 \\
0 & 0 & \beta^{11} & \beta^{5} & \beta^{9} & \beta^{2} & \beta^{3} & \beta^{6} & \beta^{1} & \beta^{12} & \beta^{10} & \beta^{3} \\
0 & 0 & 0 & 0 & \beta^{10} & \beta^{12} & \beta^{5} & \beta^{5} & \beta^{8} & \beta^{9} & \beta^{10} & 0 \\
0 & 0 & 0 & \beta^{4} & \beta^{13} & \beta^{2} & \beta^{10} & \beta^{9} & \beta^{4} & \beta^{8} & \beta^{1} & \beta^{4} \\
0 & 0 & 0 & \beta^{12} & \beta^{6} & \beta^{11} & \beta^{3} & \beta^{2} & \beta^{10} & \beta^{3} & \beta^{4} & \beta^{13} \\
0 & 0 & 0 & 0 & \beta^{7} & \beta^{1} & \beta^{5} & \beta^{13} & \beta^{1} & 0 & 0 & 0\cdots
\end{array}
$$

وبتحويل كلمات الشفرة هذه إلى النظام الثنائي نحصل على:

```
0100 1110 1001 1101 1110 0000 0000 0000 0000 0000 0000 0000
1011 1101 0111 1100 1101 0000 0000 0000 0000 0000 0000 0000
0000 1110 1100 1010 0100 1100 0000 0000 0000 0000 0000 0000
0000 1000 0101 1011 0011 0101 0000 0000 0000 0000 0000 0000
1011 1101 1110 0110 0010 0110 1010 0000 0000 0000 0000 0000
0000 0000 1110 1100 1010 0100 1100 0000 0000 0000 0000 0000
0000 1101 1101 1001 0101 1111 0010 0001 0000 0000 0000 0000
0100 0110 1100 0010 0011 1100 1101 1110 0000 0000 0000 0000
```

0000 0000 0111 1000 0010 0101 0101 0000 1101 0000 0000 0000
0000 1010 1110 0110 1001 1010 0101 1000 1100 0000 0000 0000
1011 1101 0111 0000 0111 0110 0111 1001 0011 1101 0000 0000
0000 0000 0111 0111 0110 0111 0110 1001 0001 0111 0000 0000
0000 1101 0100 0110 0110 1111 0110 1101 1001 1100 1000 0000
0000 0000 1111 1111 1111 0100 1111 1111 1010 0001 0000 0000
0000 0000 0111 0110 0101 0010 0001 0011 0100 1111 1110 0001
0000 0000 0000 0000 1110 1111 0110 0110 1010 0101 1110 0000
0000 0000 0000 1100 1011 0010 1110 0101 1100 1010 0100 1100
0000 0000 0000 1111 0011 0111 0001 0010 1110 0001 1100 1011
0000 0000 0000 0000 1101 0100 0110 1011 0100 0000 0000 0000

من الممكن الآن تحويل هذه الكلمات من كلمات طولها 4 إلى كلمات طولها 6 (على سبيل المثال، يظهر على الأقل صفر وعلى الأكثر أربعة أصفار بين كل ظهورين متتاليين للواحد) باستخدام الجدول التالي:

0000	000100	0001	010001
1000	000101	1001	101000
0100	001010	0101	101001
1100	001001	1101	101010
0010	001000	0011	100100
1010	010100	1011	100101
0110	010101	0111	100010
1110	010010	1111	100001

نضيف الآن إحداثياً بين كل كلمتين من الطول 6 (الإحداثي المضاف هو متمم لكل من الإحداثيين المجاورين). وللحفاظ على هذه الخاصية فستظهر الرسالة الأصلية m (انظر الجدول (٣،١)) على النحو التالي:

001010 1 010010 0 101000 0 101010 1 010010 1 000100 1
000100 1 000100 1 000100 1 000100 1 000100 1 000100 0 –
100101 0 101010 0 100010 1 001001 0 101010 1 000100 1
000100 1 000100 1 000100 1 000100 1 000100 1 000100 1 –
000100 1 010010 1 001001 0 010100 1 001010 1 001001 0
000100 1 000100 1 000100 1 000100 1 000100 1 000100 1 –
000100 1 000101 0 101001 0 100101 0 100100 0 101001 0
000100 1 000100 1 000100 1 000100 1 000100 1 000100 0 –
100101 0 101010 1 010010 1 010101 0 001000 1 010101 0
010100 1 000100 1 000100 1 000100 1 000100 1 000100 1 –
000100 1 000100 1 010010 1 001001 0 010100 1 001010 1
001001 0 000100 1 000100 1 000100 1 000100 1 000100 1 –
000100 0 101010 0 101010 0 101000 0 101001 0 100001 0
001000 0 010001 0 000100 1 000100 1 000100 1 000100 1 –
001010 1 010101 0 001001 0 001000 0 100100 1 001001 0
101010 1 010010 1 000100 1 000100 1 000100 1 000100 1 –
000100 1 000100 0 100010 1 000100 1 000100 0 101001 0
101001 0 000100 0 101010 1 000100 1 000100 1 000100 1 –
000100 1 010100 1 010010 1 010101 0 101000 1 010100 0
101001 0 000101 0 001001 0 000100 1 000100 1 000100 0 –
100101 0 101010 0 100010 1 000100 0 100010 1 010101 0
000100 0 101000 0 100100 0 101010 1 000100 1 000100 1 –
000100 1 000100 0 100010 0 100010 1 010101 0 100010 0
010101 0 101000 1 010001 0 100010 1 000100 1 000100 1 –
000100 0 101010 1 001010 1 010101 0 010101 0 100001 0
010101 0 101010 0 101000 1 001001 0 000101 0 000100 1 –
000100 1 000100 0 100001 0 100001 0 100001 0 001010 0
100001 0 100001 0 010100 1 010001 0 000100 1 000100 1 –
000100 1 000100 0 100010 1 010101 0 101001 0 001000 1
010001 0 100100 1 001010 0 100001 0 010010 1 010001 0 –
000100 1 000100 1 000100 1 000100 1 010010 0 100001 0

010101 0 010101 0 010100 0 101001 0 010010 1 000100 1 –
000100 1 000100 1 000100 1 001001 0 100101 0 001000 1
010010 0 101001 0 001001 0 010100 1 001010 1 001001 0 –
000100 1 000100 1 000100 0 100001 0 100100 0 100010 1
010001 0 001000 1 010010 1 010001 0 001001 0 100101 0 –
000100 1 000100 1 000100 1 000100 0 101010 1 001010 1
010101 0 100101 0 001010 1 000100 1 000100 1 000100 ?–

الملحق (د)

حلول لتمارين مختارة
Solutions to Selected Exercises

الفصل الأول: مقدمة في نظرية التشفير

(١,٢,١) (أ) 000 , 010 , 100 , 110 , 001 , 011 , 101 , 111.

(ب) 0000 , 0100 , 1000 , 1100 , 0001 , 0101 , 1001 , 1101 , 0010,0110,
1010 , 1110 , 0011 , 0111 , 1011 , 1111

(١,٢,٢) 2^n.

(١,٢,٤) يمكن تحويل القناة إلى قناة تامة باستبدال كل إحداثي 1 بالإحداثي 0 وكل إحداثي 0 بالإحداثي 1.

(١,٢,٥) استبدل كل إحداثي 0 بالإحداثي 1 وكل إحداثي 1 بالإحداثي 0.

(١,٢,٦) لا نستطيع استنتاج أي شيء عن كلمة الشفرة المرسلة من الكلمة المستقبلة.

(١,٣,٤) 001.

(١,٣,٥) $C = \{0000 , 0011 , 0101 , 0110 , 1001 , 1010 , 1100 , 1111\}$.

(أ) نعم

(ب) 0101 , 1001 , 1100 , 1111.

(ج) لا. يوجد لكل كلمة من الكلمات ذات الطول 4 التي لا تنتمي إلى الشفرة C أربع كلمات مختلفة هي الأقرب إليها.

(١,٣,٧) 8.

(١,٣,٨) 16 ، 32 ، 2^{n-1}.

(١,٤,١) 1 ، $\frac{3}{4}$ ، $\frac{1}{3}$.

(١,٦,٢) (أ) $p^3(1-p)^5 = 2 \cdot 2 \times 10^{-8}$

(ب) $p^7 = 0 \cdot 81$

(ج) $(1-p)^5 = 2 \cdot 4 \times 10^{-8}$

(د) $p^5 = 0 \cdot 86$

(هـ) $p^4(1-p)^3 = 2 \cdot 4 \times 10^{-5}$

(و) $(1-p)^5 = 2 \cdot 4 \times 10^{-8}$

(ز) $(1-p)^6 = 7 \cdot 3 \times 10^{-10}$.

(١,٦,٥) 0001110.

(١,٦,٦) 101101101.

(١,٦,٧) 00011.

(١,٦,٨) 100110.

(١,٦,٩) 110101 أو 101000.

(١,٦,١٠) (أ) $\varphi_p(v_1, w) \le \varphi_p(v_2, w)$ إذا وفقط إذا كان $d_1 \le d_2$.

(ب) $\varphi_p(v_1, w) = (\frac{1}{2})^n$ لكل w و v.

(١,٩,٥) إذا كانت أي من الكلمات 000 أو 001 أو 010 أو 011 هي المستقبلة فتستنتج طريقة IMLD أن الكلمة المرسلة هي 001. أما في الحالات المتبقية فتستنتج طريقة IMLD بصورة غير صائبة أن الكلمة المرسلة هي 101.

(١,٩,٦) فك تشفير 000 هو 000. فك تشفير كل من 001 و 011 و 101 هو 001. وفك تشفير 110 و 111 هو 110. أما بالنسبة للكلمتين 010 و 100 فيطلب إعادة إرسال.

(١,٩,٧) علامة * في الجدول التالي تعني طلب إعادة إرسال.

(أ)

الكلمة المستقبلة	فك التشفير
000	*
001	*
010	011
011	011
100	101
101	101
110	111
111	111

(ب)

الكلمة المستقبلة	فك التشفير
000	000
001	001
010	010
011	011
100	000
101	001
110	010
111	011

▲

(١,١٠,٢) (أ) $L(001) = \{000, 001, 010, 011\}$.

وبهذا نجد أن:

$$\Theta_p(C, 001) = p^3 + 2p^2(1-p) + p(1-p)^2.$$

(ب) $L(001) = \{100, 101, 110, 111\}$.

وبهذا يكون:

$$\Theta_p(C, 001) = p^3 + 2p^2(1-p) + p(1-p)^2.$$

(١,١٠,٤) (أ) $\Theta_p(C, 001) = p^3 + p^2(1-p)$.

(ب) لفك تشفير 000 تكون الكلمة المرسلة هي فقط 000، وبهذا نجد أن

$$\Theta_p(110{,}000) = p(1-p)^2.$$

(١,١٠,٥) (أ) $\Theta_p(C, 101) = p^3 + p^2(1-p)$.

(ب) $\Theta_p(C, v) = p^3 + p^2(1-p)$ لكل $v \epsilon C$.

(ج) $\Theta_p(C, 0000) = p^4 + 3p^3(1-p)$

$$\Theta_p(C, 0001) = p^4 + 3p^3(1-p)$$

$$\Theta_p(C, 1110) = p^4 + 4p^3(1-p).$$

(هـ) $\Theta_p(C, 00000) = \Theta_p(C, 11111)$

$$= p^5 + 5p^4(1-p) + 10p^3(1-p)^2$$

(ز) $\Theta_p(C,v)=p^5+3p^4(1-p)$ لكل $v\epsilon C$.

(ح) $\Theta_p(C,v)=p^6+6p^5(1-p)+9p^4(1-p)^2$ لكل $v\epsilon C$.

(**١,١١,٢**) (أ) لا (ب) نعم (ج) لا.

(**١,١١,٣**) (أ) (i) لا (ii) نعم (iii) لا.

(ب) (i) نعم (ii) نعم (iii) لا.

(**١,١١,٤**) لا يوجد.

(**١,١١,٧**) (أ) 001,011,101,111 .

(ج) $K^4\backslash\{0000,0001,1110,1111\}$.

(هـ) $K^5\backslash\{00000,111111\}$.

(ح) $K^6\backslash\{000000,101010,010101,111111\}$.

(**١,١١,١٢**) (أ) 1 (ب) 1 (ج) 1

(د) 2 (هـ) 5 (و) 3

(ز) 2 (ح) 3.

(**١,١١,١٣**) 2.

(**١,١١,١٨**) $K^3\backslash\{000,011,101,110\}$.

(**١,١١,١٩**) (أ) لا يوجد.

(د) $\{1000,0100,0010,0001\}$.

(هـ) جميع أنماط الأخطاء من الأوزان 1 ، 2 ، 3 ، 4.

(ح) جميع أنماط الأخطاء من الأوزان 1 أو 2.

(**١,١٢,١٢**) (أ) (i) 000,001 (ii) 000

(ج) (i) 0000,0010,0100,1000 (ii) 0000

(و) (i) 00000,10000,01000,00100,00010,00001

(ii) 00000,10000,01000,00100,00010,00001

(ز) (i) 00000,01000,00100,00010

(ii) 00000.

الفصل الثاني: الشفرات الخطية

(٢,١,١) الشفرتان (أ) و (ج) غير خطيّتين وباقي الشفرات هي شفرات خطيّة.

(٢,٢,٣) (أ) $\langle S \rangle = \{000\,, 010\,, 011\,, 111\,, 001\,, 101\,, 100\,, 110\}$.

(ب) $\langle S \rangle = \{0000\,, 1010\,, 0101\,, 111{,}1111\}$.

(د) $\langle S \rangle = K^4$.

(٢,٢,٧) (أ) $C^{\perp} = \{000\}$.

(ب) $C^{\perp} = \{0000\,, 1010\,, 0101\,, 1111\}$.

(ج) $C^{\perp} = \{0000\,, 1111\}$.

(٢,٣,٤) (أ) مُستقلة خطيّاً.

(ب) $\{101\,, 011\,, 010\}$.

(هـ) مُستقلة خطياً.

(ح) $\{1100\,, 1010\,, 1001\}$.

(ط) $\{10101010\,, 01010101\}$.

(٢,٣,٧) (أ) $B = \{100\,, 010\,, 001\}$ ، $B^{\perp} = \phi$.

(ب) $B = \{1010\,, 0101\}$ ، $B^{\perp} = B$.

(ج) $B = \{1010\,, 0101\,, 1100\}$ ، $B^{\perp} = \{1111\}$.

(هـ) $B = \{11000\,, 01111\,, 11110\,, 01010\}$ ، $B^{\perp} = \{11111\}$.

(٢,٣,٨) (أ) $dim\, C = 3$ ، $dim\, C^{\perp} = 0$.

(ب) $dim\, C = 2$ ، $dim\, C^{\perp} = 2$.

(ج) $dim\, C = 3$ ، $dim\, C^{\perp} = 1$.

(هـ) $dim\, C = 4$ ، $dim\, C^{\perp} = 1$.

(و) $dim\, C = 3$ ، $dim\, C^{\perp} = 2$.

(٢,٣,١٦) (أ) $dim\, C = 4$ (ب) $|C| = 16$.

(٢,٣,١٧) $|C| = 32$.

(٢,٤,١) $DC = \begin{bmatrix} 101011 \\ 110000 \\ 011011 \\ 000110 \end{bmatrix}$ $BD = \begin{bmatrix} 1000 \\ 0010 \\ 1010 \end{bmatrix}$ $BC = \begin{bmatrix} 110000 \\ 011101 \\ 101101 \end{bmatrix}$.

(٢,٤,٦) $D \leftrightarrow \begin{bmatrix} 1000 \\ 0101 \\ 0010 \\ 0000 \end{bmatrix}$ $C \leftrightarrow \begin{bmatrix} 101011 \\ 011011 \\ 000110 \\ 000000 \end{bmatrix}$ $B \leftrightarrow \begin{bmatrix} 1001 \\ 0101 \\ 0000 \end{bmatrix}$ $A \leftrightarrow \begin{bmatrix} 11011 \\ 00101 \\ 00000 \end{bmatrix}$

(٢,٥,٣) (أ) $\{100, 010, 001\}$

(ج) $\{1001, 0101, 0011\}$

(هـ) $\{100001, 01001, 00101, 00011\}$

(ز) $\{1011, 0101, 0011\}$.

(٢,٥,٦) (أ) $\{010, 011, 111\}$

(ج) $\{0101, 1010, 1100\}$

(هـ) $\{11000, 01111, 11110, 01010\}$

(ز) $\{0110, 1010, 0011\}$.

(٢,٥,١٠) (أ) ϕ

(ب) $\{1010, 0101\}$

(ج) $\{11111\}$

(د) $\{101000, 110110, 000101\}$.

(**٢,٥,١٢**) (أ) $B = \{111000\ ,000111\}$

(ب) $B = \{1000110\ ,0100011\ ,0010111\ ,0001101\}$

(ج) $B = \{1000001\ ,0100001\ ,0010001\ ,0001001\ ,0000101\ ,0000011\}$

(و) $B = \{001000\ ,000100\ ,000010\ ,000001\}$.

(**٢,٦,٤**) (i) نعم (ii) لا.

(**٢,٦,٥**) (أ) $\begin{bmatrix}010\\001\end{bmatrix}$ (ب) $\begin{bmatrix}1001\\0110\end{bmatrix}$ (د) $\begin{bmatrix}11011\\00111\end{bmatrix}$.

(**٢,٦,٦**) (أ) $dim\ C = 3$, $\begin{bmatrix}100110\\010101\\001011\end{bmatrix}$.

(**٢,٦,٧**) (أ) $(8,4,4)$, $\begin{bmatrix}10010110\\01010101\\00110011\\00001111\end{bmatrix}$ (ج) $(9,3,3)$, $\begin{bmatrix}100100100\\010010010\\001001001\end{bmatrix}$

(و) $(6,3,2)$, $\begin{bmatrix}101010\\011010\\000111\end{bmatrix}$ (ز) $(7,4,3)$, $\begin{bmatrix}1001011\\0101010\\0011001\\0000111\end{bmatrix}$

(**٢,٦,١٠**) (أ) (i) 10011 (ii) 01010 (iii) 11100.

(**٢,٦,١١**) 01011, 10011, 01011, 00101, 01110, 01011, 10110.

(**٢,٦,١٢**) (أ) 1111111, 1110100, 0001011, 1001100

(ب) 1111001, 1110101, 0001011, 0001100.

(**٢,٦,١٣**) للتمرين (**٢,٦,٦**) (أ) $|C| = 8, R = 1/2$

(ب) $|C| = 8, R = 1/3$

(ج) $|C| = 4, R = 1/5$.

وللتمرين (**٢,٦,٧**) (أ) $|C| = 16, R = 1/2$

(ب) $|C| = 16, R = 1/2$

(ج) $|C| = 8, R = 1/3$

(د) $|C| = 8, R = 3/5$

(و) $|C| = 8, R = 1/3$

(ز) $|C| = 16, R = 4/7$.

(٢,٧,٤) (أ) $\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$ (ب) $\begin{bmatrix} 01 \\ 10 \\ 10 \\ 01 \end{bmatrix}$ (ج) $\begin{bmatrix} 001 \\ 111 \\ 100 \\ 010 \\ 001 \end{bmatrix}$

(٢,٧,٥) (أ) $\begin{bmatrix} 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$ (ب) $\begin{bmatrix} 10010 \\ 01010 \\ 00101 \\ 10000 \\ 01000 \\ 00100 \\ 00010 \quad 00001 \end{bmatrix}$ (ج) $\begin{bmatrix} 1000 \\ 1000 \\ 0010 \\ 0010 \\ 0100 \\ 0100 \\ 0001 \\ 0001 \end{bmatrix}$

(ز) $\begin{bmatrix} 11 \\ 01 \\ 10 \\ 01 \\ 01 \end{bmatrix}$ (ي) $\begin{bmatrix} 111 \\ 110 \\ 101 \\ 100 \\ 011 \\ 010 \\ 001 \end{bmatrix}$.

(٢,٧,٩) (أ) $G(C^{\perp}) = G(C) = \begin{bmatrix} 110000 \\ 001010 \\ 000101 \end{bmatrix}$.

(٢,٧,١٠) تحتوي $C^{\perp}$ على 16 كلمة طول كل منها عدد زوجي في الحقل K^5.

(٢,٧,١١) (أ) $dim\, C = t\, , dim\, C^{\perp} = 2^t - t - 1\, , |C| = 2^t\, ,$
$|C^{\perp}| = 2^{2^t - t - 1}\, , R = t/(2^t - 1)$

(ب) $dim\, C = 11\, , dim\, C^{\perp} = 12\, , |C| = 2^{11} = 2048\, ,$
$|C^{\perp}| = 2^{12} = 4096\, , R = 11/23$

(ج) $dim\, C = 8\, , dim\, C^{\perp} = 7\, , |C| = 2^8 = 256\, ,$
$|C^{\perp}| = 2^7 = 128\, , R = 8/15$.

(٢,٨,٤) (أ) 1111100 (ب) 1011000.

(٢,٨,١٠) (أ) $C' = \{00000\, , 11100\, , 10101\, , 01001\}$.

(٢,٨,١١) (أ) $G' = \begin{bmatrix}100011\\010010\\001001\\000100\end{bmatrix}$.

(٢,٨,١٢) (أ) $G' = \begin{bmatrix}10110\\01011\end{bmatrix}$.

(٢,٨,١٤) (أ) نعم (ب) نعم (ج) لا.

(٢,٩,٤) (أ) 4 (ب) 4 (ج) 4.

(٢,١٠,٦) (أ) $C, C+1000, C+0010, C+0011$

(ب) $C, C+1000, C+0100, C+0001$.

(٢,١٠,٧) (أ) $C, C+100000, C+010000, C+001000, C+000100,$
$C+000010, C+000001, C+001001$

(د) $C, C+100000$

(و) $C, C+1000, C+0100, C+0010, C+0001,$
$C+1100, C+1010, C+1001$.

(٢,١٠,٨) (أ) $C, C+1000, C+0100, C+0001$

(ب) $C, C+1000000, C+0100000, C+0010000, C+0001000,$
$C+0000100, C+0000010, C+0000001$

(ج) $C, C+000100, C+010000, C+001100, C+100000,$
$C+100100, C+110000, C+110100$

(٢,١١,٢) (أ) 010011 (ب) 101001 (ج) 001111

(د) 010011 (هـ) 110101 (و) 001111.

(٢,١١,٨)

(أ)

التناذر	نمط الخطأ
11	*
00	0000
01	*
10	0010

، $H = \begin{bmatrix}01\\01\\10\\01\end{bmatrix}$.

(**٢,١١,٩**)

(أ)

التناذر	نمط الخطأ
000	000000
001	000001
010	000010
011	100000
100	000100
101	010000
110	001000
111	*

، $H = \begin{bmatrix} 011 \\ 101 \\ 110 \\ 100 \\ 010 \\ 001 \end{bmatrix}$.

(**٢,١١,١٠**)

(ب)

التناذر	نمط الخطأ
000	0000000
001	0000001
010	0000010
011	0001000
100	0000100
101	0010000
110	0100000
111	1000000

(**٢,١١,١٩**) (أ) (i) 1100 (ii) 1001 (iii) 0101

(ج) (i) 001110 (ii) 001110 (iii) 011011.

(**٢,١١,٢١**)

(أ)

التناذر	نمط الخطأ
000	0000000
001	0000001
010	0000010
011	0001000
100	0000100
101	0010000
110	0100000
111	1000000

(**٢,١٢,٢**) للتمرين (**٢,١٠,٦**) (أ) $\theta_p(C) = p^4 + p^3(1-p)$.

(ج) $\theta_p(C) = p^5 + 3p^4(1-p)$.

وللتمرين (**٢,١٠,٧**) (أ) $\theta_p(C) = p^6 + 6p^5(1-p)$.

(ب) $\theta_p(C) = p^6 + 6p^5(1-p) + 9p^4(1-p)^2$.

وللتمرين (٢,١٠,٨) (أ) $\theta_p(C) = p^4 + 2p^3(1-p)$.

(ب) $\theta_p(C) = p^7 + 7p^6(1-p)$.

الفصل الثالث: الشفرات التامة والشفرات ذات الصلة بها

(٣,١,٥) (أ) 2^4 (ب) 2^4 (ج) 2^4

(هـ) 2^8 (و) 4096.

(٣,١,١٨) (أ) (8,6,3) ، لا ، $16 \leq |C| \leq 16$

(د) (15,6,3) ، نعم ، 2048.

(٣,١,١٩) (أ) $64 \leq |C| \leq 256$ (ب) $2048 \leq |C| \leq 2048$

(ج) $128 \leq |C| \leq 128$ (د) $256 \leq |C| \leq 256$

(هـ) $32 \leq |C| \leq 256$ (و) $16 \leq |C| \leq 32$.

(٣,١,٢٠) لا.

(٣,٣,٤)

التناذر	نمط الخطأ
000	0000000
111	1000000
110	0100000
101	0010000
011	0001000
100	0000100
010	0000010
001	0000001

$$H = \begin{bmatrix} 111 \\ 110 \\ 101 \\ 011 \\ 100 \\ 010 \\ 001 \end{bmatrix}$$

(أ) 0101011 (ج) 0011110.

(٣,٤,٧) (أ) 696 (ب) 17 (ج) 17.

(٣,٦,٥) (أ) 100000001001, 000000000000

(ب) 000000100000, 001000010000

(ج) 000000100000 , 000000010000

(د) اطلب إعادة ارسال.

(هـ) 00000000100 , 011000000000

(ز) 001010000000 , 000000000000.

(٣,٦,٦) (أ) 000000000000 , 010010000000

(ب) 001000110000 , 000000000000

(ج) 100000000000 , 001000000000

(د) 000000000001 , 000000000101

(هـ) 000110000000 , 000100000000

(و) 000000001000 , 000001000000.

(٣,٧,٣) (أ) 10101111011 , 111111100000

(ب) 11011100010 , 100000000000

(ج) 11100000000 , 000101011001

(د) 011011011011 , 011000001001.

(٣,٧,٧) 253.

(٣,٨,٥)
$$\begin{bmatrix} 1111 & 1111 \\ 0101 & 0101 \\ 0011 & 0011 \\ 0001 & 0001 \\ 0000 & 1111 \\ 0000 & 0101 \\ 0000 & 0011 \end{bmatrix}$$

(٣,٨,١٠) (أ) 1010 0101 (ب) 0110 0110

(ج) اطلب إعادة ارسال. (د) 1100 1100

(٣,٩,٦) (أ) $m = (0101)$ $w_3 = (2,-2,2,-2,-2,-6,-2,2)$.

(ب) $m = (0110)$ $w_3 = (2,-2,-2,-6,-2,2,2,2)$.

(ج) $m = ?$ $w_3 = (-4,-4,0,0,0,0,-4,4)$.

(د) $m = (1010)$ $w_3 = (2,2,6,-2,-2,-2,2,2)$.

الفصل الرابع: الشفرات الخطية الدورية

(٤,١,١٠) (أ) $q(x) = x^3, r(x) = x^3$.

(٤,١,١٣) (أ) $\{0 + x^2, x, x + x^2\}$ (ج) $\{0, x^3, 1 + x + x^2\}$.

(٤,٢,٢٢) (أ) $g(x) = 1$ (هـ) $g(x) = 1 + x$.

(٤,٣,٥) (أ) $\begin{bmatrix} 1011000 \\ 0101100 \\ 0010110 \\ 0001011 \end{bmatrix}$.

(٤,٣,٦) (ب) $\begin{bmatrix} 101010 \\ 010101 \end{bmatrix}$ $g(x) = 1 + x^2 + x^4$.

الفصل الخامس: شفرات BCH

(٥,١,١٥)

(أ) $\begin{bmatrix} 00 & 0 \\ 10 & \beta^0 \\ 01 & \beta \\ 11 & \beta^2 \end{bmatrix}$ (ب) $\begin{bmatrix} 000 & 0 \\ 100 & \beta^0 \\ 010 & \beta \\ 001 & \beta^2 \\ 101 & \beta^3 \\ 111 & \beta^4 \\ 110 & \beta^5 \\ 011 & \beta^6 \end{bmatrix}$.

(٥,١,١٧) $\beta, \beta^2, \beta^4, \beta^7, \beta^8, \beta^{11}, \beta^{13}, \beta^{14}$.

(٥,٢,٧)

كثيرة الحدود الأصغرية	العنصر
x	0
$1 + x$	1
$1 + x + x^3$	β, β^2, β^4
$1 + x^2 + x^3$	β, β^6, β^5

(٥,٢,٨)

كثيرة الحدود الأصغرية	العنصر
x	0
$1 + x$	1
$1 + x + x^2$	β^5, β^{10}
$1 + x + x^4$	$\beta^7, \beta^{14}, \beta^{13}, \beta^{11}$
$1 + x^3 + x^4$	$\beta, \beta^2, \beta^4, \beta^8$
$1 + x + x^2 + x^3 + x^4$	$\beta^3, \beta^6, \beta^9, \beta^{12}$

(**٥,٢,٩**) (أ) اطلب إعادة ارسال. (ب) 10.

(ج) 5 و 8. (د) 6 و 11.

(هـ) اطلب إعادة ارسال. (و) اطلب إعادة ارسال.

(ز) 0 و 13. (ح) كلمة شفرة.

الفصل السادس: شفرات ريد وسولومن

(**٦,١,٦**) (أ) 2^{15}.

(ب) $g(x) = \beta + \beta^3 x + x^2$.

(ج) (i) $\beta\beta\beta^6\beta^6 000$.

(د) $g_k(x) = (1 + x)(\beta + x)(\beta^2 + x)(\beta^4 + x)$.

(**٦,١,٧**) (أ) 2^{44}.

(ب) $g(x) = \beta^{10} + \beta^3 x + \beta^6 x^2 + \beta^{13} x^3 + x^4$.

(ج) (i) $\beta^{10}\beta^3\beta^6\beta^{13}100000\beta^2\beta^{10}\beta^{13}\beta^5\beta^7$.

(د) $g_k(x) = (\beta^8 + x)(\beta^6 + x)(\beta^{12} + x)(\beta^9 + x)g(x)$.

(**٦,٢,٣**) (أ) β^2 (ب) β^5 (ج) β^4.

(**٦,٢,٧**) (أ) $n = 3, k = 1, d = 3$ و $|C| = 4$

(ب) $G = [\beta\beta^2 1]$

(ج)

$f(c)$	الرسالة	كلمة الشفرة c
000000	0	0 0 0
011110	1	$\beta\ \beta^2\ 1$
111001	β	$\beta^2\ 1\ \beta$
1001111	β^2	$1\ \beta\ \beta^2$

(**٦,٢,٨**) (أ) $n = 7, k = 3, d = 5$ و $|C| = 8^3 = 512$.

(ب) $g(x) = \beta^6 + \beta^5 x + \beta^5 x^2 + \beta^2 x^3 + x^4$.

(٦,٢,٩) (أ) $(\beta + x)(1 + x) = (\beta^4 + x)(\beta^3 + x) = \beta + \beta^2 x + x^2$.

(ب) $(\beta^4 + x)(\beta^3 + x) = 1 + \beta^6 x + x^2$.

(ج) $(\beta^4 + x)(\beta^3 + x)(\beta^2 + x)(\beta + x) = \beta^3 + \beta x + x^2 + \beta^3 x^3 + x^4$

(د) $\beta^{10} + \beta^3 x + \beta^6 x^2 + \beta^3 x^3 + x^4$
$= (\beta + x)(\beta^2 + x) + (\beta^3 + x)(\beta^4 + x)$

(ج) $\beta^{21} + \beta^{24} x + \beta^{16} x^2 + \beta^{24} x^3 + \beta^9 x^4 + \beta^{10} x^5 + x^6$
$= (\beta + x)(\beta^2 + x) \cdots (\beta^6 + x)$

(٦,٣,٥) (أ) $00\beta\beta^5\beta^3\beta^2\beta^{13}\beta^{10}\beta000000$

(ب) $1\beta^4\beta^2\beta\beta^{12}\beta^9 10\beta\beta^5\beta^3\beta^2\beta^{13}\beta^{10}\beta$

(ج) $\beta\beta^{10}\beta^7 0\beta^{12}\beta^3\beta^3 10000000$.

(٦,٣,٦) (أ) $001\beta^8\beta^{11}\beta^3\beta^5 00000000$

(ب) $0\beta^{10}\beta^3\beta^6\beta^{13} 0\beta^8\beta^{11}\beta^3\beta^5 00000$

(ج) $\beta^4\beta^{12} 1\beta^7 0\beta^2\beta^5\beta^{12}\beta^{14} 000000$.

(٦,٣,٨) (أ) $0\beta^2 0000000000000$

(ب) $00\beta 00\beta^3 000000000$

(ج) 100000000000000

(د) $\beta^5 11100000000000$

(هـ) $\beta^{10}\beta^3 0001000010000$

(و) $\beta^2 0000\beta^2 0000\beta^2 0000$.

(٦,٥,٤) (أ) $(\beta + x)$

(ب) $(\beta^3 + x)(\beta^2 + x)$

(ج) $(\beta^{10} + x) + (\beta^5 + x)$

(د) $(1+x)(\beta+x)(\beta^2+x)(\beta^3+x)$

(هـ) $(1+x)(\beta+x)(\beta^5+x)(\beta^{10}+x)$

(و) $(1+x)(\beta^5+x)(\beta^{10}+x)$

في الجدول التالي، لكل p_i و q_i يمثل الرمز * عنصر الحقل الصفري والرمز i يمثل العنصر β^i.

(أ)

−1	0	2	3	4	5	6	7	8	9				0	−1	−∞
0	2	3	4	5	6	7	8	9				0	*	0	−1
1	7	8	9	10	11	12	13				0	2	*	1	0
2	*	*	*	*	*	*				0	1	*	*	2	1
3	*	*	*	*	*				0	1	*	*	*	4	1
4	*	*	*	*				0	1	*	*	*		6	1
5	*	*	*				0	1	*	*	*			8	1
6	*	*				0	1	*	*	*				10	1
7	*				0	1	*	*	*					12	1
8				0	1	*	*	*						(14)	(1)

$$\sigma(x) = x + \beta^1$$

(ب)

−1	0	9	13	7	4	12	4	8	2				0	−1	−∞
0	9	13	7	4	12	4	8	2				0	*	0	−1
1	8	*	0	1	12	3	*				0	9	*	1	0
2	12	13	9	0	*	7				0	4	*	*	2	1
3	13	14	10	1	*				0	*	13	*	*	3	2
4	*	*	*	*				0	1	7	*	*		4	3
5	*	*	*				0	1	7	*	*			6	3
6	*	*				0	1	7	*	*				8	3
7	*				0	1	7	*	*					10	3
8				0	1	7	*	*						(12)	(3)

$$\sigma(x) = x^2 + \beta^1 x + \beta^7 = (x+\beta^2)(x+\beta^5)$$

(ج)

−1	0	0	0	0	0	0	0	0	0				0	−1	−∞
0	0	0	0	0	0	0	0	0				0	*	0	−1
1	*	*	*	*	*	*	*				0	0	*	1	0
2	*	*	*	*	*	*				0	0	*	*	3	0
3	*	*	*	*	*				0	0	*	*	*	5	0
4	*	*	*	*				0	0	*	*	*		7	0
5	*	*	*				0	0	*	*	*			9	0
6	*	*				0	0	*	*	*				11	0
7	*				0	0	*	*	*					13	0
8				0	0	*	*	*						(15)	(0)

$$\sigma(x) = x + \beta^0$$

(د)

−1	0	10	3	13	3	12	5	13	3				0	−1	−∞
0	10	3	13	3	12	5	13	3				0	*	0	−1
1	11	*	13	1	13	6	13				0	10	*	1	0
2	4	2	0	*	*	2				0	8	*	*	2	1
3	2	13	9	6	13				0	*	3	*	*	3	2
4	6	10	6	13				0	13	2	*	*		4	3
5	4	0	9				0	11	2	7	*			5	4
6	2	14				0	4	9	9	*				6	5
7	2				0	11	*	7	5					7	6
8				0	12	4	0	6						(8)	(7)

$$\begin{aligned}\sigma(x) &= x^4 + \beta^{12}x^3 + \beta^4x^2 + \beta^0x + \beta^6 \\ &= (x+\beta^0)(x+\beta^1)(x+\beta^2)(x+\beta^3)\end{aligned}$$

(هـ)

−1	0	12	8	*	7	13	4	13	0				0	−1	−∞
0	12	8	*	7	13	4	13	0				0	*	0	−1
1	12	5	7	11	2	12	5				0	12	*	1	0
2	4	7	8	14	6	7				0	11	*	*	2	1
3	2	6	0	5	3				0	8	4	*	*	3	2
4	9	13	14	7				0	3	14	*	*		4	3
5	*	1	2				0	4	3	11	*			5	4
6	1	2				0	4	3	11	*				7	4
7	1				0	4	4	14	6					6	6
8				0	1	*	0	1						(8)	(7)

$$\begin{aligned}\sigma(x) &= x^4 + \beta^1x^3 + \beta^0x + \beta^1 \\ &= (x+\beta^1)(x+\beta^0)(x+\beta^5)(x+\beta^{10})\end{aligned}$$

(و)

-1	0	2	*	*	2	*	*	2	*				0	-1	$-\infty$
0	2	*	*	2	*	*	2	*				0	*	0	-1
1	4	*	2	4	*	2	4				0	2	*	1	0
2	*	2	*	*	2	*				0	*	*	*	2	1
3	2	*	*	2	*				0	*	*	*	*	4	1
4	*	0	*	*				0	*	13	0	*		3	3
5	0	*	*				0	*	13	0	*			5	3
6	*	*				0	*	*	0	*				6	3
7	*				0	*	*	0	*					8	3
8				0	*	*	0	*						(10)	(3)

$\sigma(x) = x^3 + 1 = (x + \beta^0)(x + \beta^5)(x + \beta^{10})$.

(٦,٦,٩) (أ) 0000 0000 1001 0011 1111 1111 1010

(ب) 1001 0011 1010 0011 0000 1010 1001

(ج) 0101 1100 1001 1100 0000 1001 0101

(د) 0000 1001 0011 1111 1111 1010 0000.

(٦,٦,١٠) فك تشفير $f(w)$ ليكون $f(c)$ حيث c هي :

(أ) $\beta^{10}\beta^{12}\beta^{7}\beta^{3}\beta^{12}\beta^{8}\beta^{8}\beta^{2}0000000$

(ب) $\beta^{10}0\beta\beta^{7}\beta^{7}0\beta^{0}\beta^{2}0000000$

(ج) $0\beta^{12}\beta^{14}\beta^{4}\beta^{2}\beta^{8}\beta^{2}00000000$.

(٦,٦,١١) فك تشفير $\bar{f}(w)$ ليكون $\bar{f}(c)$ حيث $c = \beta^{7}\beta^{7}1\beta^{9}\beta\beta^{10}\beta^{8}10000000$.

الفصل السابع: شفرات تصويب الأخطاء الاندفاعية

(٧,١,٥) C ليست شفرة تصويب خطأين ؛ لأن عدد مجموعاتها المشاركة يساوي 32.

(٧,١,٦) C ليست شفرة تصويب ثلاثة أخطاء ؛ لأن عدد مجموعاتها المشاركة يساوي 64.

(**٧,١,١٣**) (أ) 101100000001000

(ج) 100000101010011

(هـ) 00000111100100 .

(**٧,١,١٤**) (أ) 010100000010010

(ج) 001110000000100

(هـ) 000000011111010 .

(**٧,٢,٤**) (أ) 1000110 0110110 1110000 0011100 0110110 0001111

(ب) 10 01 01 00 11 11 00 10 10 11 01 01 00 00 00 10 10 01 11 11 01

(ج) 101 011 011 000 110 110 000 000 010 110 101 111 011 001.

(**٧,٢,٨**) (أ) 1 ****** 00 ***** 110 **** 0110 *** 00101 ** 011011 *

(ب) 1 ****** 0 ****** 10 ***** 01 ***** 010 **** 001 ****.

(**٧,٢,٩**) يتم ارسال كلمات الشفرة بالترتيب دون توريق.

(**٧,٢,١٢**) (أ) 01 10 11 11 10 01 10 11 11 01 01 00 01 00 11 01
10 11 10 10 11 00 01 01

(ب) 011 101 111 110 100 010 001 100 111 101 110 011.

(**٧,٢,١٣**) (أ) $m_1 = 0000, m_2 = 0011, m_3 = 0000$

(ب) $m_1 = 1000, m_2 = 0110, m_3 = 0011$.

الفصل الثامن: شفرات التلاف

(**٨,١,٧**) (أ) $11101001\cdots$ (ب) $0010111\cdots$.

(**٨,١,١٢**) (أ) 000 , 0010000 (ب) 001 , 1110000.

(**٨,١,١٤**) (أ) 000 , 0010000 (ب) 000 , 100 .

(٨,٢,٢) (أ) $c(x) = (1 + x + x^4 + x^6, 1 + x + x^2 + x^4 + x^5 + x^6, 1 + x^2 + x^5 + x^6)$

(ب) $c(x) = (1 + x^2 + x^6, 1 + x^3 + x^5 + x^6, 1 + x + x^2 + x^3 + x^4 + x^5 + x^6)$

(ج) $c(x) = (1 + \sum_{i=3}^{\infty} x^i, 1 + x^2, 1 + x + \sum_{i=3}^{\infty} x^i)$.

(٨,٢,٣) (أ) $c(x) = (1 + x + x^2 + x^3 + x^6, 1 + x^2 + x^5 + x^6)$

(ب) $c(x) = (1 + x + x^5 + x^6 + x^7, 1 + x^7)$

(ج) $c(x) = (1 + x^2 + \sum_{i=1}^{\infty} x^{2i+1}, 1 + x + \sum_{i=3}^{\infty} x^i)$.

(٨,٢,٦) صيغة التوريق لكلمات الشفرة هي :

للتمرين **(٨,٢,٢)** (أ) ⋯ 111 110 011 000 110 011 111

(ب) ⋯ 111 001 101 011 001 011 111

(ج) ⋯ 111 001 010 101 101 101 101.

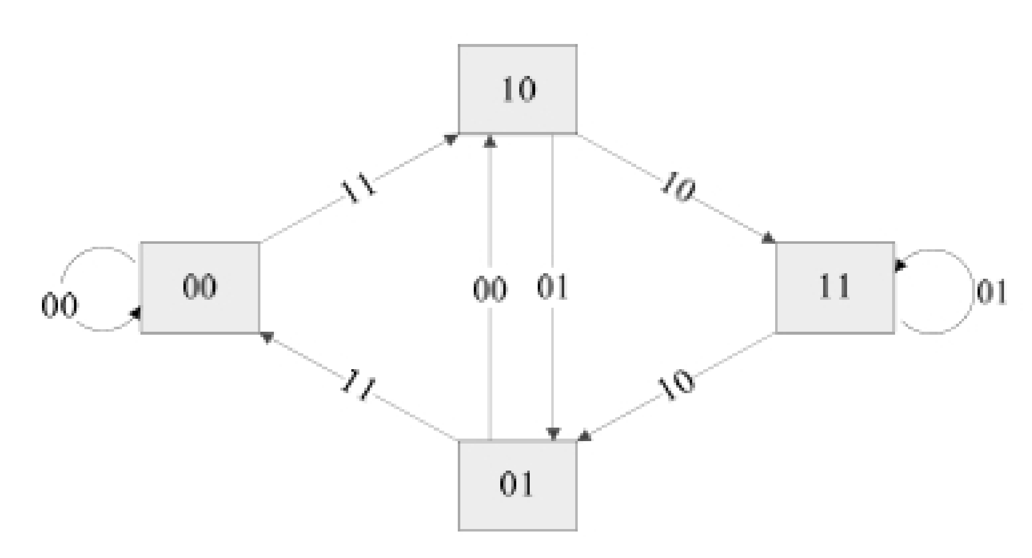
وللتمرين **(٨,٢,٣)** (أ) ⋯ 11 10 11 10 00 01 11

(ب) ⋯ 11 10 00 00 00 10 10 11

(ج) ⋯ 11 01 10 11 01 11 01 11 01 .

(٨,٢,١١)

(أ)

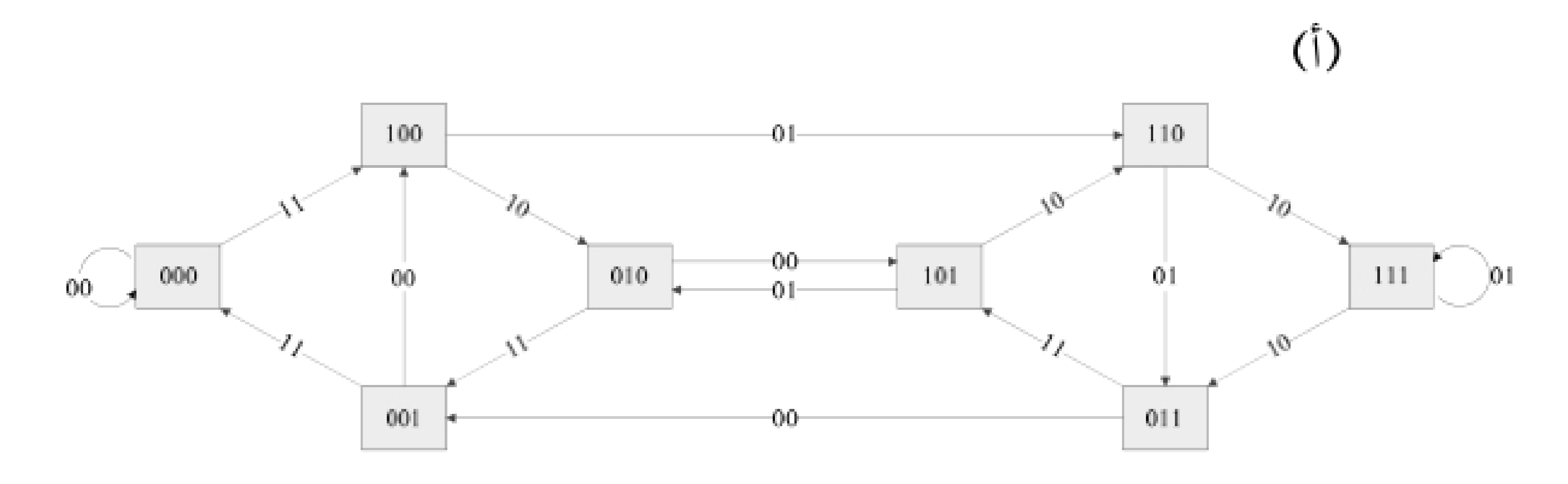


(ب) (i) ⋯ 11 01 00 01 11 00 00 (ii) ⋯ 11 10 01 10 11 00 00

(ج) (i) ⋯ 1 0 1 0 0 0 (ii) ⋯ 0 1 1 1 1 0 1.

(٨,٢,١٢)

(أ)



(ب) (i) ⋯ 00 00 11 11 10 00 11 10 11

(ii) ⋯ 00 00 11 11 01 11 01 01 11

(iii) ⋯ 01 01 01 10 01 11

(ج) (i) ⋯ 1 1 1 0 1 0 1

(ii) ⋯ 0 0 1 1 1 1 0.

(٨,٣,١) (أ) $m = 1010101 \cdots = \sum_{i=1}^{\infty} x^{2i}$

(ب) $\cdots * 1 * 1 * 1$

(ج) $\cdots 000 *$

(٨,٣,٢) (أ) $gcd = 1 + x$ والعروة على المرحلة 111 هي دورة وزنها صفر.

(ب) $gcd = 1$ وهي ليست شفرة اخفاق تام.

(ج) $gcd = 1 + x + x^2$ ، (0110,1011,1101) دورة وزنها صفر.

(٨,٣,٣) (أ) 5 (ب) 6 (ج) 7.

(٨,٣,٦) (أ) $\tau(a) = 2, \tau(2) = 6$

(ب) $\tau(1) = 2, \tau(2) = 6$

(ج) $\tau(1) = 2, \tau(2) = 9, \tau(3) = 13$.

(٨,٤,٤)

المرحلة s	$t=8$	$t=9$	$t=10$	$t=11$	$t=12$
000	$3{,}00000**$	$3{,}000000*$	$3{,}0000000$	$3{,}0000000$	$3{,}0000000$
100	$5{,}100****$	$3{,}1001001$	$5{,}100****$	$3{,}1001110$	$5{,}100****$
010	$4{,}0100100$	$4{,}0101001$	$4{,}0100100$	$4{,}0101110$	$4{,}0100111$
110	$4{,}1100100$	$4{,}1101001$	$4{,}1100100$	$4{,}1101110$	$4{,}1100111$
001	$3{,}0010011$	$5{,}001****$	$3{,}0011100$	$5{,}001***0$	$5{,}001*1*1$
101	$3{,}1010011$	$5{,}101****$	$3{,}1011100$	$5{,}101***0$	$5{,}101*1*1$
011	$4{,}011*0**$	$2{,}0111001$	$4{,}0111*0*$	$4{,}0111010$	$5{,}0111001$
111	$2{,}1110011$	$4{,}111*0**$	$4{,}1110100$	$4{,}1110010$	$4{,}1110111$
فك التشفير	1	1	0	0	0

(٨,٤,٥) (أ) $m = 0\,0\,0$ (ب) $m = 1\,0\,0$.

(٨,٤,١٤) (ب)

المرحلة s	المخرج $X_3=0$	$X_3=1$	$t=1$	2	3	4	5	6	7	8
000	00	11	∞	∞	∞	7	6	6	6	6
100	11	00	2	∞	∞	5	4	5	5	6
010	10	01	∞	3	∞	4	6	5	6	6
110	01	10	∞	3	∞	4	6	5	6	6
001	11	00	∞	∞	5	4	5	5	6	6
101	00	11	∞	∞	3	6	4	6	5	6
011	01	10	∞	∞	4	5	5	6	6	7
111	10	01	∞	∞	4	5	5	6	6	7

$d = 6, \tau(1) = 2, \tau(2) = 6$

الفصل التاسع: شفرات ريد ومولر وبريبراتا

(٩,١,٣) (أ) $f_I(x) = (x_0+1)(x_3+1)$

(ب) $v_I = 1000100000000000, f_I(x) = (x_0+1)(x_1+1)(x_3+1)$

(ج) $f_I(x) = (x_1+1)$

(د) $v_I = 1111000000000000, f_I(x) = (x_2+1)(x_3+1)$

(هـ) $v_I = 1, f_I(x) = 1$

(و) $100 \cdots 0, f_I(x) = \prod_{i=0}^{3}(x_i+1)$.

(**٩,١,٤**) (أ) $f_I(x) = (x_0+1)(x_4+1)$

(ج) $f_I(x) = (x_1+1)$

(د) $f_I(x) = (x_1+1)(x_2+1)(x_4+1)$

(هـ) $v_I = 11 \cdots 1, f_I(x) = 1$

(و) $v_I = 100 \cdots 0, f_I(x) = \prod_{i=1}^{4}(x_i+1)$.

(**٩,١,٥**) يوجد عدد $|I|$ من الإحداثيات الصفرية وخياران لكل من الإحداثيات الأخرى التي عددها $m-|I|$ في H_I.

(**٩,١,٦**) بما أن أوزان جميع v_I (عدا v_{I_m}) زوجية فنرى أن وزن v زوجي إذا وفقط إذا كان $v\epsilon\langle v_{I_m}\rangle^{\perp}$.

(**٩,١,٩**) (أ)
$$\begin{bmatrix} 11111111 \\ 11110000 \\ 11001100 \\ 10101010 \\ 11000000 \\ 10100000 \\ 10001000 \end{bmatrix} \begin{matrix} v_\emptyset \\ v_2 \\ v_1 \\ v_0 \\ v_{1,2} \\ v_{0,2} \\ v_{0,1} \end{matrix}$$

(**٩,١,١٢**) (أ) $c = v_2 + v_0 = 0101\ \ 1010\ \ 1010\ \ 1010$

(ب) $c = v_{0,1} = 1000\ \ 1000\ \ 1000\ \ 1000$

(ج) $c = v_2 + v_{0,3} = 0101\ 1010\ 1111\ 0000$.

(**٩,٢,٧**) (أ) 0 1000 000001 (ب) 0 0000 0 11000

(ج) 1 1001 100000 (د) 1 1111 111111

(هـ) 0 0100 000100 (و) 0 0101 010000

(ز) 0 0000 000010 (ح) 0 0110 00000

(ط) 1 0001 000101.

(**٩,٢,٨**) (أ) 0 00000 0000000100 (ب) 0 00100 1000100001

(ج) 1 00000 0000010000 (د) 1 00100 1100000000

(هـ) 0 01001 0000000100 (و) 0 10010 0000000000

(ز) اطلب اعادة ارسال.

(**٩,٣,١٠**) (أ) (ii) 1001 1010 11110011 (iii) 01100101 11110011

(ج) (ii) 11000110 10101111 (iii) 11001001 11100111.

(**٩,٣,١١**) (أ) إذا كان $\alpha = 0$ فنرى أن $\alpha U = \{0\}$ ومن ثم $|\alpha U|$ عدد فردي. من ذلك نرى أن $[\chi(U), \chi(V)]$ لا تحقق الشرط (i) من التعريف (**٣,٣,٩**).

(**٩,٣,١٧**) (أ) 01000001 01110100 (ب) 00001001 01001110

(ج) 00000011 11010010.

(**٩,٤,٦**) (أ) 10101001 11011011 (ب) 10101001 00100100

(ج) 11111111 11111111 (د) 11111111 00000000

(هـ) 00000000 11111111.

(**٩,٤,٧**) (أ) $0 \cdots 00000100010 \; 0 \cdots 10100$ (ب) $0 \cdots 00 \; 0 \cdots 10100$.

(**٩,٤,٨**) (أ) 31 (ب) 21.

(**٩,٥,٣**) (أ) 1000001 11101000 (ب) 00011110 01000010

(ج) 00000101 10100110 (د) 01000010 00011110

(هـ) 11101000 10000001 (و) 10011011 01111101

(ز) اطلب إعادة إرسال (ح) 10100101 10010000

(ط) 11101101 01010101 (ي) 10111011 01101010

(ك) 11101101 01010101 (ل) 10111011 01101010

(م) 10010000 10100101.

(**٩,٥,٤**) (أ) 11000 00011 11 10000 00000 00000 10000 11000 11000
00 00100 00011 01000 00000

(ب) 10001 00000 00 00000 00000 00000 00000 00000 10100
00 10111 01010 00000 00000

(**٩,٥,٥**) لا.

الفصل العاشر: التعمية التقليدية

(**١٠,٢,٥**) تقترح الكلمة "VHV" بأن طول المفتاح يقسم 16. وبما أن النص المعمى للنص الواضح 'an' هو 'AE' فنرى أن جزءاً من كلمة المفتاح هو 'AR'. بعد إثبات أن طول المفتاح يجب أن يكون أكبر من 2، أدرس الحالة التي تفترض أن طول المفتاح يساوي 4. المعلومات التي تحصل عليها من الجزء 'AE' تؤدي إلى أن المفتاح يجب أن يكون "?AR?" حيث علامة الاستفهام تعني حرف غير معلوم. الآن استخدم المعلومات التي تتعلق أزواج من كلمات مكررة مكونة من ثلاثة حروف لتخمين كلمة المفتاح.

(**١٠,٢,٨**) توجد سيناريوات تدعى أن الضغط المتبوع بتعمية يساعد على كسر النظام (على سبيل المثال، إذا استخدم الضغط على رأس مقدمة مخرجات معلوم فمن الممكن كسر النظام باستخدام معرفة النص الواضح ويعتمد ذلك على نظام التعمية المستخدم). والاقتراح العام هو إجراء عملية الضغط أولاً. يمكن أن يكون الضغط أكثر فاعلية على النص الواضح منه على النص المعمى. إذا كانت عملية التعمية أو ارسال المعلومات مكلفة فإن اجراء

الضغط أولاً قد يؤدي إلى تحسين العملية. كما أن عملية الضغط قبل التعمية يمكن أن تخلق صعوبات لمحاولة الكسر المبنية على تذيل المصدر. انظر بويد (Boyd [16]) والمصادر الأخرى المذكورة فيه.

(١٠,٣,١) $m = (m_0, m_1) = (1110, 0000)$

(١٠,٣,٣) $m_1 = m_3 \oplus f_{k_2}(m_2) = 1010 \oplus f_1(1010) = 0000$
$m = (m_0, m_1) = (1110, 0000)$

(١٠,٣,٤) (أ) كشف المعمى في CBC هو $m_i = \mathrm{DES}_k^{-1}(c_i) \oplus c_{i-1}$ فقط m_j و m_{j+1} يعتمدان على c_j.

(١٠,٣,٥) (أ) لاحظ أن $k_2 = \mathrm{DES}_{k_1}(m) \oplus E_k(m)$ لكل $0 \leq i < 2^{56}$ ضع $j = \mathrm{DES}_i(m_1) \oplus c_1$. إذا كان $\mathrm{DES}_i(m_2) \oplus j = c_2$ فمن المرجح أن يكون $(i, j) = (k_1, k_2)$. نحتاج على الأكثر إلى 2^{57} عملية DES لإيجاد مرشحاً.

(١٠,٣,٧) ليس معلوماً أن خاصية أخذ المتمم تحسن من استنفاذ المفاتيح لكسر النظام بطريقة معرفة النص الواضح فقط. أما في حالة استخدام طريقة اختيار النص الواضح، احصل على زوجين (m, c_1) و $(\overline{m}, c_2)$ واستخدم خاصية أخذ المتمم لحذف مفتاحين مرشحين مع كل عملية DES.

الفصل الحادي عشر: مواضيع في الجبر ونظرية الأعداد

(١١,١,١٤) باستخدام الخوارزمية **(١١,١,٧)** حيث $n = 576$ نجد أن:

i	0	1	2	...	8
k_i	0	0	1	...	1
A	47	$47^2 \bmod n = 481$	$481^2 \bmod n = 385$	...	$193^2 \bmod n = 385$
b	1	1	$1 \cdot 385 \bmod n = 385$	...	$385 \cdot 385 \bmod n = 193$

ومن ثم يكون $47^{332} \equiv 193 (\bmod 576)$.

(**١١,١,١٦**) يمكن إيجاد مجموعة المولدات $\{2,6,7,8\}$ بحسابات مباشرة، على سبيل المثال:

$$2^2 \equiv 4 \text{ ،} \quad 2^4 \equiv 4 \cdot 4 \equiv 5 \text{ ،} \quad 2^5 \not\equiv 1 .$$

ومن ثم فإن رتبة 2 تساوي 10 ؛ لأن رتبة العنصر يجب أن تقسم $\varphi(11) = 10$. إذا كان α مولّداً للزمرة $\mathbb{Z}_n^*$ فمن الممكن أثبات أن α^i مولّداً إذا وفقط إذا كان $(i, \varphi(n)) = 1$. من ذلك نرى أنه إذا كانت $\mathbb{Z}_n^*$ دورية فإن عدد المولّدات يساوي $\varphi(\varphi(n))$. في هذا التمرين عدد المولّدات هو $\varphi(\varphi(11)) = \varphi(10) = 4$ وهي 2^i حيث $i \in \{1,3,7,9\}$.

(**١١,١,٢١**) (أ) استخدم خوارزمية القسمة لكتابة:

$$x = q \cdot ord(a) + r \text{ حيث } 0 \le r < ord(a).$$

لنفرض أن $a^x \equiv 1 (\bmod n)$. عندئذ،

$$1 \equiv a^{q \cdot ord(a) + r} \equiv a^r (\bmod n)$$

وبما أن $r < ord(a)$ فنرى استناداً إلى تعريف الرتبة أن $r = 0$. وبهذا يكون $ord(a) \mid x$.

(**١١,١,٢٢**) استخدم وجود مولّداً للزمرة $\mathbb{Z}_p^*$ و التمرين (**١١,١,٢٠**).

(**١١,٢,٧**) احسب قيمة $x^2 (\bmod 30)$ لكل $x \in \mathbb{Z}_{30}^* = \{1,7,11,13,17,19,23,29\}$ لتحصل على $Q_{30} = \{1,19\}$. يكفي أن تجري الحسابات حيث $x < \frac{30}{2}$ ؛ لأن $n - x \equiv -x (\bmod n)$.

(**١١,٢,٨**) $\left(\frac{156}{235}\right) = -1$ و

$$\left(\frac{1833}{587}\right) = \left(\frac{72}{587}\right) = \left(\frac{2^3 \cdot 3^2}{587}\right) = \left(\frac{2}{587}\right)^3 \left(\frac{3}{587}\right)^2 = -1 .$$

(١١,٢,١٣) استخدم معيار أويلر.

(١١,٣,٥) إذا لم يكن a شاهداً لأويلر فإن:

$(a,n) = 1$ وأن $a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) (\bmod n)$.

احسب مربع كل من مقادير التطابق.

من الممكن تصميم لاختبار أن العدد مؤلف باستخدام شاهد فيرما ولكن توجد أعداد مؤلفة n (تسمى أعداد كارمايكل) بحيث لا يكون لها أي شاهد فيرما في المجموعة $\mathbb{Z}_n^*$.

(١١,٤,٥) $m = \left\lfloor \sqrt{n} \right\rfloor = 32$ و $q(z) = (z+32)^2 - 1081$.

أساس التحليل هو $B = \{-1, 2, 3, 5, 11\}$ لأن $\left(\frac{n}{7}\right) = -1$. الجدول التالي يقدم بعض قيم z بحيث يتحلل $q(z)$ على B.

z	$a = z + m$	$b = q(z)$	التحليل
-1	31	-120	$-2^3 \cdot 3 \cdot 5$
1	33	8	2^3
2	34	75	$3 \cdot 5^2$
-3	29	-240	$-2^4 \cdot 3 \cdot 5$

العلاقات للقيم تؤدي إلى $x^2 \equiv y^2 (\bmod n)$ حيث $x = 31 \cdot 33 \cdot 29$ و $y = 2^5 \cdot 3 \cdot 5$. ولسوء الحظ $x \equiv 480 \equiv y (\bmod n)$. ولا توجد تركيبات أخرى تؤدي إلى مربع كامل، ولهذا نحتاج لتوليد قيم أخرى.

(١١,٤,٦) ظهرت هذه المسألة في [63]. وجدت قيم x و y التي تحقق تقابل $z \in \{0, 1, -2\}$ و $z \in \{-1, 4, -6\}$. القيم الأولى منها تؤدي إلى أن $x \equiv -y$.

(١١,٤,٨) لاحظ أن $179 \equiv 3 (\bmod 11)$ وأن $179 \equiv 9 (\bmod 17)$. وبما أن $11 \equiv 3 (\bmod 4)$ فالتطابق $x^2 \equiv 3 (\bmod 11)$ له الحلان $x = \pm 3^{(11+1)/4}$.

وعلى الرغم من عدم تقديمنا خوارزمية لحل التطابق $x^2 \equiv 9 \pmod{17}$ إلا أنه يمكن وبسهولة إيجاد الحلين بالتجريب وهما $x \equiv \pm 3 \pmod{17}$. باستخدام خوارزمية جاوس نجد أن 71 هو أحد الجذور التربيعية للعدد 179.

(١١,٤,١٠) يمكن حساب قيمة $p+q$ بمعرفة n و φ. الآن، ادرس المعادلة $(x-p)(x-q)=0$.

(١١,٥,٣) الجدول التالي يبين قيم الأزواج (j, α^j):

j	0	1	2	3	4	5	6	7	8	9
$\alpha^j \bmod p$	1	5	25	28	43	21	8	40	6	30

وبحساب $\beta\alpha^{-im} \bmod p$ حتى الحصول على تقابل نجد أن:

$$\begin{aligned}
i = o: &\quad \beta(\alpha - m)^0 \equiv \beta \equiv 4 \\
i = 1: &\quad \beta(\alpha - m)^1 \equiv 4 \cdot 11 \equiv 44 \\
i = 2: &\quad \beta(\alpha - m)^2 \equiv 44 \cdot 11 \equiv 96 \\
i = 3: &\quad \beta(\alpha - m)^3 \equiv 96 \cdot 11 \equiv 86 \\
i = 4: &\quad \beta(\alpha - m)^4 \equiv 86 \cdot 11 \equiv 73 \\
i = 5: &\quad \beta(\alpha - m)^5 \equiv 73 \cdot 11 \equiv 27 \\
i = 6: &\quad \beta(\alpha - m)^6 \equiv 27 \cdot 11 \equiv 6
\end{aligned}$$

إذن $\beta\alpha^{-im} \equiv \alpha^j$ حيث $i=6$ و $j=8$ ولهذا يكون $\log_5 4 = 68 \in \mathbb{Z}_{97}$.

(١١,٥,٦) (أ) بوضع $\lambda = 2^i \lambda'$ حيث λ' فردي نستطيع افتراض أن $2^i \mid \varphi(p)$ دون المساس بالعمومية. اعتبر الآن عنصراً $a \in \mathbb{Z}_n^*$ من الرتبة $\varphi(p)$ كعنصر ينتمي إلى $\mathbb{Z}_p^*$ ومن الرتبة $\frac{\varphi(q)}{2}$ كعنصر ينتمي إلى $\mathbb{Z}_q^*$.

(ب) أثبت أن $\lambda = ord(a)\lambda'$ وأن $x = 2^i ord(a) x'$ لأعداد $i \geq 0$، λ'، x' حيث λ' فردي. عندئذ يكون:

$$a^{\lambda/2} \equiv a^{ord(a)\lambda'/2} \equiv a^{ord(a)/2} \equiv a^{x/2^{i+1}} \pmod n.$$

الفصل الثاني عشر: أنظمة التعمية ذوات المفتاح المعلن

(١٢,١,٧) يمكن أن يقوم العدو بحساب $h(kxy) = f(M, y)$ لكل قالب y.

(١٢,١,٨) لاحظ أن $2pq \mid (x_i - x_j)$. إذا كان على سبيل المثال، $d = (x_1 - x_2, x_1 - x_3) < n$ فنكون قد وجدنا $2pq$ أو $4pq$. وبما أن $n = (2p + 1)(2q + 1)$ فمن الممكن أن نجد الآن بطريقة فعالة على p و q بمعرفة n و d.

(١٢,٢,٢) (أ) استخدم خوارزمية إقليدس لإيجاد $d = 233$.

(ب) استخدم الخوارزمية **(١١,١,٧)** لإثبات أن:

$c \equiv m^e (\bmod pq) \equiv 921 (\bmod pq)$.

(١٢,٢,٣) من الممكن الإجابة على هذا التمرين مباشرة باستخدام الصيغة التي تحسب عدد الرسائل ذاتية التعمية. بصورة عامة لأي عدد قياس $n = pq$ لنظام ESA من السهل الاثبات على وجود قوة e بحيث تحقق $1 < e < \varphi(n)$، $(e, \varphi(n)) = 1$، $m^e \equiv m (\bmod n)$ لكل m.

ضع $e = 1 + j\varphi(n) / (p - 1, q - 1)$ حيث $1 \leq j < (p - 1, q - 1)$. التمرين هو الحالة $j = (p - 1, q - 1) / 2$.

(١٢,٢,٤) لنظام التطابقات $x \equiv c_i (\bmod n_i)$ الحل $x < n_1 n_2 n_3$. بما أن $m < n_i$ فنجد أن $x = m^3$. من الممكن إيجاد الجذر التكعيبي للعدد x بطريقة فعالة لنحصل على m (في الحالة النادرة التي تكون فيها القياسات ليست أولية نسبياً مثنى مثنى نقوم بتحليل القياسات أولاً).

(١٢,٢,٦) (أ) إذا كان $k < 1$ فإن $1 = ed - k\varphi(n) \geq ed$ ومن ثم نحصل على تناقض. بما أن $d < \varphi(n)$ فنجد أن $1 = ed - k\varphi(n) < (e - k)\varphi(n)$ وأن $k < e$.

(ب) $1 = ed - k\varphi(n) = ed - k(n - p - q + 1)$.

وبهذا يكون:

$$.\frac{kn+1}{e} - d = \frac{k}{e}(p+q-1) < p+q$$

(١٢,٢,٧) (أ) $.n - \varphi(n) = n - (n-p-q+1) < p+q < 3\sqrt{n}$

(ب) $$\left|\frac{e}{n} - \frac{k}{d}\right| = \left|\frac{ed-kn}{dn}\right| < \frac{k(n-\varphi(n))}{dn}$$
$$< \frac{3k}{d\sqrt{n}} < \frac{1}{3d^2}$$

(ج) احسب أقرب تقريب للعدد $\frac{k'}{d'}$ إلى $\frac{e}{n}$. من التحقق من العدد d' بإيجاد φ' من $ed' - k'\varphi' = 1$ ومن ثم (بحالة $\varphi' \in \mathbb{Z}$) حاول تحليل العدد n باستخدام التمرين (**١٠,٤,١١**).

(١٢,٢,١٠) إذا كان $ed \equiv 1(\bmod \lambda)$ فإن $ed \equiv 1(\bmod p-1)$ وأن $m^{ed} \equiv m(\bmod p)$. وبالمثل، $m^{ed} \equiv m(\bmod q)$. وبهذا يكون $m^{ed} \equiv m(\bmod n)$. لاحظ أن $\lambda \mid \varphi(n)$. وبهذا فإن استخدام λ يمكن أن يؤدي إلى عدد d أصغر. وإذا اخترنا p و q عشوائياً فمن المتوقع أن يكون $(p-1, q-1)$ صغيراً.

(١٢,٢,١١) (أ) مماثل تقريباً للتمرين (**١٢,٢,١٠**).

(ب) $\lambda = 12$، $\varphi(n) = 48$، $\varphi(p,q) = 84$، $.\lambda \mid \varphi(p,q)$

(١٢,٢,١٣) اختار رسالة $m > p$ ثم احسب $c \equiv m^e(\bmod n)$ ليكون النص المعمى المختار.

(١٢,٤,٢) (أ) $x = 9$ و $.(r,s) = (7,13)$

(١٢,٥,٣) (ب) إذا كان من التوقع هو $e = 1$ فإن الخيارين $X = S$ و $y = 1$ سيحققان شرط التحقيق المقابل على الغم من أن الشهادة من هذه الجلسة ستظهر أنها غير حقيقية. وبدلاً من ذلك خذ الخيار $X = S^x$.

المراجع
Bibliography

[1] Derek Atkins, Michael Graff, Arjen K. Lenstra, and Paul C. Leyland. The magic words are squeamish ossifrage. In Josef Pieprzyk and Reihanah Safavi-Naini, editors, *Advances in Cryptology –ASIACRYPT '94*, volume 917 of *Lecture Notes in Computer Science*, pages 263-277. Springer-Verlag, 1995.

[2] Eric Bach. Discrete logarithms and factoring. Technical Report UCB/CSD 84/186, University of California Berkeley, Computer Science Division, June 1984.

[3] Henry Beker and Fred Piper, *Cipher Systems: The Protection of Communication*. J. Wiley & Sons, New York, 1982.

[4] Mihir Bellare and Phillip Rogaway. Optimal asymmetric encryption. In Alfredo De Santis, editor, *Advances in Cryptology –EUROCRYPT '94*, volume 950 of *Lecture Notes in Computer Science*, pages 92-111. Springer-Verlag, 1995. A revised version is available via http://www.cse.ucsd.edu/users/mihir/.

[5] E.R. Berlekamp. *Algebraic Coding Theory.* McGraw-Hill, 1968.

[6] R.E. Blahut. *Theory and Practice of Error Control Codes*. Addison-Wesley, 1983.

[7] I. F. Blake and R. C. Mullin. *An Introduction to Algebraic and Combinational Coding Theory*. Academic Press, 1976.

[8] Ian F. Blake, G. Seroussi, and Nigel P. Smart. *Elliptic Curves in Cryptography*, volume 265 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, 1999.

[9] Matt Blaze, Whitfield Diffie, Ronald L. Rivest, Bruce Schneier, Tsutomu Shimomura, Eric Thompson, and Michael Wiener. Minimal key lengths for symmetric ciphers to provide adequate commercial security: A report by an ad

hoc group of cryptographers and computer scientists. Available through http://www.bsa.org/, January 1996.

[10] Daniel Bleichenbacher. Generating ElGamal signatures without knowing the secret key. In Maurer [59], pages 10-18. A revised version correcting Corollary 2 is available from the Information Security and Cryptology Research Group, ETH-Zurich, ftp://ftp.inf.ethz.ch.

[11] M. Blum. Coin flipping by telephone: a protocol for solving impossible problems. In *Proceedings of the 24th IEEE Computer Conference (CompCon)*, pages 133-137, 1982.

[12] Dan Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the AMS*, 46(2):203-213, February 1999. Available via http://theory.stanford.edu/~dabo/.

[13] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. On the importance of checking cryptographic protocols for faults. In Fumy [35], pages 37-51. The extended abstract is expanded in "On the importance of eliminating errors in cryptographic computations", available via http://thory.stanford.edu/~dabo/.

[14] Dan Boneh and Glenn Durfee. New results on the cryptanalysis of low exponent RSA. In J. Stern, editor, *Advances in Cryptology – EUROCRYPT '99*, volume 1592 of *Lecture Notes in Computer Science*, pages 1-11. Springer-Verlag, 1999. Available via http://theory.stanford.edu/~dabo/.

[15] Dan Boneh and Ramarathnam Venkatesan. Breaking RSA may be easier the factoring. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT ' 98*, volume 1403 of *Lecture Notes in Computer Science*, pages 59-71. Springer-Verlag, 1998. Available via http://theory.stanford.edu/~dabo/.

[16] Colin Boyd. Enhancing security by data compression: theoretical and practical aspects. In D. W. Davies, editor, *Advances in Cryptology – EUROCRYPT '91*, pages 267-280. Springer-Verlag, 1991.

[17] Gilles Brassard, editor. *Advances in Cryptology – CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*. Springer-Verlag, 1989.

[18] Gilles Brassard, and Claude Crépeau. Sorting out zero- knowledge. In J. J. Quisquater and J. Vandewalle, editors, *Advances in Cryptology – UROCRYPT '89*, volume 434 of *Lecture Notes in Computer Science*, pages 181-191. Springer-Verlag, 1990.

[19] David Chaum, Jan-Hendrik Evertse, Jeroen van de Graaf. An improved protocol for demonstrating possession of discrete logarithms and some generalizations. In David Chaum and Wyn L. Price, editors, *Advances in Cryptology – EUROCRYPT '87*, volume 304 of *Lecture Notes in Computer Science*, pages 127-141. Springer-Verlag, 1988.

[20] David Chaum, Jan-Hendrik Evertse, Jeroen van de Graaf, and René Peralta. Demonstrating possession of a discrete logarithm without revealing it. In

Andrew M. Odlyzko, editor, *Advances in Cryptology – CRYPTO '86*, volume 263 of *Lecture Notes in Computer Science*, pages 200-212. Springer-Verlag, 1987.

[21] Clifford C. Cocks. A note on 'non-secret encryption'. Technical report, Communication Electronics Security Group (CESG), November 1973. Available via http://www.cesg.gov.uk.

[22] Don Coppersmith. Cheating at mental poker. In Williams [98], pages 104-107.

[23] Don Coppersmith. The Data Encryption Standard (DES) and its strength against attacks. *IBM Journal of Research and Development*, 38(3):243-250, May 1994.

[24] Don Coppersmith, Mathew Franklin, Jacques Patarin, and Michael Reiter. Low-exponent RSA with related messages. In Maurer [59], pages 1-9.

[25] Richard A. DeMillo, Georgie I. Davida, David P. Dobkin, Michael A. Harrison, and Richard J. Lipton. *Applied Cryptology, Cryptographic Protocols, and Computer Security Models*. Proceedings of Symposia in Applied Mathematics. American Mathematical Society, Providence, 1983. Lecture notes for the AMS short course. *Cryptology in Revolution: Mathematics and Models*, San Francisco, 1981.

[26] Whitfield Diffie, The first ten year of public key cryptography. In Simmons [81], chapter 3, pages 135-175.

[27] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644-654, 1976.

[28] Whitfield Diffie and Martin E. Hellman. Exhaustive cryptanalysis of the NBS Data Encryption Standard. *Computer*, 10(6): 74-84, June 977.

[29] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE Transactions of Information Theory*, 31(4):469-472, July 1985.

[30] J. H. Ellis. The possibility of secure non-secret digital encryption. Technical report, Communications Electronics Security Group (CESG), January 1970. Available via http://www.cesg.gov.uk.

[31] J. H. Ellis. The history of non-secret encryption. Technical report, Communications Electronics Security Group (CESG), December 1997. Available via http://www.cesg.gov.uk.

[32] David C. Feldmeier and Philip R. Karn. Unix password security – ten years later. In Brassard [17], pages 44-63.

[33] Steven Fortune and Michael Merritt. Poker protocols. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology – CRYPTO '84*, volume 196 of *Lecture Notes in Computer Science*, pages 454-464. Springer-Verlag, 1985.

[34] Electronic Frontier Foundation. *Cracking DES: Secrets of Encryption Research, Wiretap Politics, and Chip Design*. Distributed by O'Reilly and Associates, 1998.

[35] Walter Fumy, editor. *Advances in Cryptology – EUROCRYPT '97*, volume 1233 of *Lecture Notes in Computer Science*. Springer-Verlag, 1997.

[36] R.G. Gallager, *Information Theory and Reliable Communication*. John Wiley and Sons, 1968.

[37] Simon Garfinkel. *PGP: Pretty Good Privacy*. O'Reilly & Associates, 1995.

[38] W. J. Gilbert. *Modern Algebra with Applications*. Wiley, 1976.

[39] Ian Goldberg and David Wagner. Randomness and the Netscape Browser. *Dr. Dobb's Journal*, pages 66-70, January 1996.

[40] Shafi Goldwasser, Silvio Micali, and Charles Rackoff. The knowledge complexity of interactive proof systems. *SIAM journal on Computing*, 18(1):186-208, February 1989.

[41] Martin Handford. *Where's Waldo?* Little, Brown, Boston, 1987.

[42] G.H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford Clarendon Press, second edition, 1945.

[43] R. Hill. *A First Course in Coding Theory*. Oxford University Press, 1986.

[44] Don Johnson and Alfred Menezes. The Elliptic Curve Digital Signature Algorithm (ECDSA). CORR 99-134, University of Waterloo, Canada, August 1999. Available from http://cacr.math.uwaterloo.ca.

[45] D. S. Jones. *Elementary Information Theory.* Oxford University Press, 1979.

[46] Antoine Joux and Reynald Lercier. State-of-the-art in implementing algorithms for the (ordinary) discrete logarithm problem. The 3rd workshop on Elliptic Curve Cryptography (ECC '99), University of Waterloo, http://www.cacr.math.uwaterloo.ca, November 1-3 1999.

[47] Marc Joye, Arjen K. Lenstra, and Jean-Jacques Quisquater. Chinese remaindering based cryptosystems in the presence of faults. *Journal of Cryptology*, 12(4):241-245, Autumn 1999.

[48] David Khan. *The Codebreakers: The Story of Secret Writing*. Scribner, New York, revised edition, 1996.

[49] Joe Kilian and Phillip Rogaway. How to protect DES against exhaustive key search. In Koblitz [51], pages 252-267. Available via http://www.cs.ucdavis.edu/~rogaway/; a summary appears in [73].

[50] Neal Koblitz. *A Course in Number Theory and Cryptography*. Springer, second edition, 1994.

[51] Neal Koblitz, editor. *Advances in Cryptology – CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.

[52] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, *Advances in Cryptology – CRYPTO '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 388-397. Springer-Verlag, 1999.

[53] Paul C. Kocher. Timing attacks on implementations of Diffie-Hellman, RSA, DES and other systems. In Koblitz [51], pages 105-113.

[54] B. A. LaMacchia and A. M. Odlyzko. Computation of discrete logarithms in prime fields. *Designs, Codes and Cryptography*. 1(1):47-62. May 1991.

[55] Arjen K. Lenstra and Eric R. Verheul. Selecting cryptographic key sizes. The 3rd workshop on Elliptic Curve Cryptography (ECC '99), University of Waterloo, http://www.cacr.math.uwaterloo.ca, November 1-3 1999.

[56] R. Lidl and H. Neiderreiter. *Finite Fields*. Cambridge University Press, 1984.

[57] S. Lin and D. J. Costello, Jr. *Error Control Coding: Fundamentals and Applications*. Prentice-Hall, 1983.

[58] F. J. MacWilliams and J. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[59] Ueli Maurer, editor. *Advances in Cryptology EUROCRYPT '96*, volume 1070 of *Lecture Notes in Computer Science*. Springer-Verlag, 1996.

[60] R. J. McEliece. *The Theory of Information and Coding*. Addison-Wesley, 1977.

[61] R. J. McEliece. *Finite Fields for Computer Scientists and Engineers*. Kluwer Academic Publishers, 1987.

[62] Alfred J. Menezes. *Elliptic Curve Public Key Cryptosystems*, volume 234 of *Kluwer international series in engineering and computer science*. Kluwer Academic Publishers, 1993.

[63] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, 1996. Errata and a complete on-line copy of the book are available on http://www.cacr.math.uwaterloo.ca/hac/.

[64] J. H. Moore. Protocol failures in cryptosystems. In Simmons [81], chapter 11, pages 541-558.

[65] Moni Naor, Yael Naor, and Omer Reingold. Applied kid cryptography, or how to convince your children that you are not cheating. CRYPTO '98 rump session, August 1998.

[66] W. W. Peterson and E. J. Weldon, Jr. *Error-Correcting Codes*. MIT Press, 1972.

[67] V. Pless. *Introduction to the Theory of Error-Correcting Codes*, Wiley, 1982.

[68] Jean-Jacques Quisquater, Louis Guillou, and Tom Berson. How to explain zero-knowledge protocols to your children. In Brassard [17], pages 628-631.

[69] M. O. Rabin. Digitalized signatures and public-key functions as intractable as factorization. Technical Report 212, MIT Laboratory for Computer Scientists, 1979.

[70] Rick Ramsey. *All About Administering NIS+*. SunSoft, second edition, 1994.

[71] Ronald L. Rivest. Cryptography. In van Leeuwen [91], pages 719-755.

[72] Ronald L. Rivest, and Adi Shamir. How to expose an eavesdropper. *Communications of the ACM*, 27(4):393-395, April 1984.

[73] Phillip Rogaway. The security of DESX. *CryptoBytes*, 2(2):8-11, Summer 1996. RSA Laboratories newsletter, http://www.rsa.com. The article is a summary of [49].

[74] Kenneth H. Rosen. *Elementary number Theory and its Applications*. Addison-Wesley, third edition, 1993.

[75] Arto Salomaa. *Public-Key Cryptography*. Texts in theoretical computer science. Springer-Verlag, second edition, 1996.

[76] Bruce Schneier. *Applied Cryptography: protocols, algorithms, and source code in C*. John Wiley & Sons, Inc., second edition, 1996.

[77] Jennifer Seberry and Josef Pieprzyk. *Cryptography: an introduction to computer security*. Prentice Hall, 1989.

[78] Adi Shamir. RSA for paranoids. *CryptoBytes*, 1(3):1-4, Autumn 1995. RSA Laboratories newsletter, http://www.rsa.com.

[79] Adi Shamir, Ronald L. Rivest, and Leonard M. Adelman. Mental poker. In David A. Klarner, editor, *The Mathematical Gardner*, pages 37-43. Prindle, Weber, and Schmidt, Boston, 1981.

[80] C. E. Shannon. A mathematical theory of communications. *Bell System Technical Journal*, 27:379-423 and 623-56, 1948.

[81] G. J. Simmons, editor. *Contemporary Cryptology: the science of information integrity*. IEEE Press, 1992.

[82] Gustavus J. Simmons. The prisoners' problem and the subliminal channel. In David Chaum, editor *Advances in Cryptology – CRYPTO '83*, pages 51-67, New York, 1984. Plenum Press.

[83] Gustavus J. Simmons. The subliminal channel and digital signatures. In Thomas Beth, Norbert Cot, and Ingemar Ingemarsson, editors, *Advances in Cryptology – EUROCRYPT '84*, volume 209 of *Lecture Notes in Computer Science*, pages 364-378.Springer-Verlag, 1985.

[84] Gustavus J. Simmons. Subliminal channels; past and present. *European Transactions on Telecommunications,* 5(4):459-473, July – August 1994.

[85] Gustavus J. Simmons. Subliminal communication is easy using DSA. In Tor Helleseth, editor, *Advances in Cryptology – EUROCRYPT '93*, volume 765 of *Lecture Notes in Computer Science*, pages 218-232. Springer-Verlag, 1994.

[86] Douglas R. Stinson. *Cryptography: Theory and Practice*. CRC Press, Boca Raton, Florida, 1995.

[87] Robert Sugarman. On foiling computer crime. *IEEE Spectrum*, 16(7):31-32, July 1979. This is the first of a series of articles: Martin E. Hellman, DES will be total insecure within ten years, 32-39; Security Agency denies tampering with DES, National Security Agency, 39; George I. Davida, Hellman's scheme breaks DES in its basic form, National Science Foundation, 39; Walter Tuchman, Hellman presents no shortcut solution to the DES, 40-41; Dennis Branstad, Hellman's data does not support his conclusion, National Bureau of Standards, 41.

[88] Bradley Taylor and David Goldberg. Secure networking in the Sun environment. Technical Report 905, Sun Microsystems, January 1991.

[89] A. Tietäväinen. On the nonexistence of perfect codes over finite fields. SIAM *Journal on Applied Mathematics,* 24:88-96,1973.

[90] Malcolm Turnbull. *The Spycatcher Trial: the scandal behind the #1 best seller*. Salem house Publishers, 1989. See [101].

[91] J. van Leeuwen, editor. *Handbook of Theoretical Computer Science*. Elsevier Science Publishers, 1990.

[92] J. H. van Lint. *Introduction to Coding Theory*. Springer- Verlag, 1982.

[93] Michael Wiener. Efficient DES key search. In W. Stallings, editor, *Practical Cryptography for Data Internetworks*, pages 31-79. IEEE Computer Society Press, 1996. Reprinted from Crypto 93 rump session.

[94] Michael Wiener. Efficient DES key search – an update. In *Cracking DES* [34], chapter 11, pages 1-4.

[95] Michael J. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory*, 36(3):553-558, May 1990.

[96] H. C. Williams. A modification of the RSA public-key encryption procedure. *IEEE Transactions on Information Theory*, 26(6):726-729, November 1980.

[97] H. C. Williams. An M^3 public-key encryption scheme. In Williams [98], pages 358-368.

[98] Hugh C. Williams, editor, *Advances in Cryptology – CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*. Springer-Verlag, 1985.

[99] Malcolm J. Williamson. Non-secret encryption using a finite field. Technical report, Communications Electronics Security Group (CESG), January 1974. Available via http://www.cesg.gov.uk.

[100] Malcolm J. Williamson. Thoughts on cheaper non-secret encryption. Technical report, Communication Electronics Security Society (CESG), August 1976. Available via http://www.cesg.gov.uk.

[101] Peter Wright. *Spycatcher: the candid autobiography of a senior intelligence officer*. Viking, New York, 1987. See also [90].

[102] Adam Young and Moti Yung. The dark side of "black-box" cryptography, or: should we trust Capstone. In Koblitz [51], pages 89-103.

[103] Adam Young and Moti Yung. Kleptography: using cryptography against cryptography. In Fumy [35], pages 62-74.

[104] Philip R. Zimmermann. *The Official PGP User's Guide*. MIT Press, Cambridge, Massachusetts, 1995.

[105] V. Zinoviev and V. Leontiev. The nonexistence of perfect codes over Galois fields. *Problems of Control and Information Theory*, 2(2):16-24, 1973.

ثبت المصطلحات

Glossary

أولاً: عربي – إنجليزي

أ

Primality testing	اختبار الأوليات
Solovay-Strassen test	اختبار سولوفي وستراسن
Kasiski test	اختبار كاسيكي
Miller-Rabin test	اختبار ميلر ورابن
Random choice	اختيار عشوائي
Chosen-ciphertext	اختيار نص معمى
Chosen-plaintext	اختيار نص واضح
Axhaustive keyspace	استنفاد فضاء المفاتيح
Pseudosquares	أشباه المربعات
Modes of operations	أشكال العمليات
The integers	الأعداد الصحيحة
The integers odulo n	الأعداد الصحيحة قياس n

الأمن القابل للبرهان	Provable security
التعمية المتكررة	Multiple encryption
التعمية ذات المفتاح المتماثل	Symmetric-key encryption
الخطوة الصغيرة	Baby-step
الخطوة الكبيرة	Giant-step
الخوارزميات	Algorithms
الرواسب التربيعية	Quadratic residues
الرواسب غير التربيعية	Quadratic nonresidues
العدو (حواء)	Adversary (Eve)
القاسم المشترك الأكبر	Greatest common divisor
اللوغاريتمات المنفصلة	Discrete logarithms
المحافظة على السر	Confidentiality
المرسل (أليس)	Sender (Alice)
المرشح التربيعي	Quadratic sieve
المستقبل (بوب)	Receiver (Bob)
المضاعف المشترك الأصغر	Least common multiple
النشر	Diffusion
النص المعمى	Ciphertext
النص الواضح	Plaintext
آمن برهاناً	Provably secure
آمن تماماً	Unconditionally secure

آمن حسابياً	Computationally secure
انتحال الشخصية	Impersonation
انتروبيا	Entropy
أنظمة السيل	Stream ciphers
أنظمة المرحلة	State ciphers
أنظمة تعمية قالبية	Block ciphers
أوليان نسبياً	Relatively prime

ب

بذرة بدائية	Initial seed
برتوكول الثلاث خطوات لشامير	Shamir's 3-pass protocol
برتوكولات تعموية	Cryptographic protocols
بطاقة ذكية	Smartcard

ت

تحليل الأعداد	Factoring of numbers
تحليل التردد	Frequency analysis
تحليل التعمية	Cryptanalysis
تذيل (تمليح) الرسالة	Salting the message
تركيب خطي	Linear combination
تزوير الرسالة	Forgery
تزوير وجودي	Existential forgery
تشويش	Confusion

تعقد الحسابات	Complexity
تعمية تقليدية	Classical cryptography
تعمية سلسلة قوالب	Cipher-block chaning
تعمية فينونا	VENONA
توقيع الجمل	ELGamal signature
توقيع إلكتروني	Digital signature
توقيع إلكتروني مع ملحق	Digital signature with appendix
توليد مفتاح	Key generating

ج

جذور تربيعية	Square roots

ح

حساب التطابقات	Moduler arithmetic
حساب الدليل	Index calculus
حلقة	Ring
حواشي	Notes

خ

خصوصية جيدة وبارعة	Pretty good privacy (PGP)
خصوصية سيئة جداً	Pretty awful privacy
خطة توقيع نظام RSA	RSA Signature scheme
خطط التعمية	Encryption schemes
خطط المفتاح المتماثل	Symmetric-key schemes

Euclidean algorithm	خوارزمية إقليدس
Extended Euclidean algorithm	خوارزمية إقليدس الموسعة
Square and multiply algorithm	خوارزمية التربيع والضرب
Secure hash	خوارزمية التموية الآمنة
Division algorithm	خوارزمية القسمة
Gauss algorithm	خوارزمية جاوس
Polynomial time algorithm	خوارزمية حدودية
Efficient algorithm	خوارزمية فعالة

د

Encryption function	دالة التعمية
Euler function	دالة أويلر
Hash function	دالة تمويه
Cryptographic hash function	دالة تمويه تعموية
One-way function	دالة ذات اتجاه واحد
Trapdoor function	دالة ذات باب سري
Decryption function	دالة كشف المعمى

ر

Order of integer	رتبة عدد صحيح
Message digest	رسالة ملخصة
Big-oh notation	رمز O الكبيرة
Jacobi symbol	رمز جاكوبي
Legendre symbol	رمز ليجندر

ز

زمرة	Group

س

سلامة البيانات	Date integrity
سلطة الشهادات	Certification authority
سلم فيستل ملتو	Feistel twisted ladder

ش

شاهد أويلر	Euler witness
شاهد فيرما	Fermat witness
شاهد قوي	Strong witness
شفرة اكتشاف معدلة	Modification detection code
شفرة توثيق الرسالة	Message authentication code
شفرة مطابقة هوية الرسالة	Message authentication code
شكل رو	Rho-diagram
شهادة	Certificate

ض

ضغط البيانات	Data compression
ضم (تسلسل)	Concatenation

ط

طريقة الالتقاء بالمنتصف	Meet-in-the-middle attack
طريقة رو لبولارد	Pollard's rho method
طول القالب	Block length

ع

عدد أولي	Prime number
عدد مؤلف	Composite number
عدم الإنكار (التنصل)	Nonrepudiation
عدم المعرفة مطلقاً	Zero-knowledge
عدو غير فعال	Passive adversary
عدو فعال (نشط)	Active adversary
علم التعمية	Cryptology
عملية الفصل المتنافية (XOR)	Exclusive or (XOR)

ف

فصل تطابق	Congruence class
فصل تكافؤ	Equivalence class
فضاء الرسائل	Message space
فضاء المفاتيح	Key space

ق

قابل للعكس	Invertible
قانون المقلوب التربيعي	Low of quadratic reciprocity
قناة اتصال	Communication channel
قناة آمنة	Secure channel
قناة غير آمنة	Nonsecure channel
قناة مخفية	Subliminal channel

قوة شاملة	Universal exponent
قيمة عشوائية	Random value

ك

كتاب التعمية الإلكتروني	Electronic cod book
كلمة سر	Password
كلمة سر (مفتاح)	Secret word (key)

ل

لفافة لمرة واحدة	One-time pad

م

مبرهنة الأعداد الأولية	Prime number theorem
مبرهنة الباقي الصينية	Chinese remainder theorem
مبرهنة أويلر	Euler's theorem
مبرهنة فيرما الصغرى	Fermat's little theorem
مثنى مثنى	In pairs
محاولات بيرنولي	Bernoulli trials
مربعات عشوائية	Random squares
مرشح الحقل العددي	Number field sieve
مسألة الجذور التربيعية	SQROOT
مسألة الجمل	ELGAMAL
مسألة الرواسب التربيعية	QRP
مسألة اللوغاريتم المنفصل	DLP

مسألة تحليل الأعداد الصحيحة	FACTOR
مسألة حساب Φ	COMPUTE Φ
مسألة ديفي وهيلمان	DHP
مسألة رابن	RABIN
مطابقة الهوية الشخصية	Identification
مطابقة هوية الرسالة	Message authentication
معامل الصدفة	Index of coincidence
معرفة النص المعمى فقط	Cipher text-only
معرفة النص الواضح	Known-plaintext
معكوس (نظير) ضربي	Multiplicative inverse
معيار أويلر	Euler's criterion
منع التزوير	Non-repudiation
موثوقية (تطابق الهوية)	Authentication
مولِّد	Generator

ن

نظام RSA	RSA cipher
نظام أحادي	Monoalphabetic cipher
نظام الازاحة	Shift cipher
نظام البيانات الجديد المحكم	New data seal (NDS)
نظام التعمية القياسي المتقدم	Advanced encryption standard (AES)
نظام الجمل	ELGamal
نظام القيصر	Ceasar cipher

نظام تطابقات	Congruence system
نظام تعددي	Polyalphabetic cipher
نظام تعمية البيانات القياسي	Date encryption standard (DES)
نظام تعمية ذو مفتاح معلن	Public-key cryptography
نظام تعمية فيرنام	Vernam cipher
نظام تعمية فيستل	Feistel cipher
نظام تعويض بسيط	Simple substitution cipher
نظام رابن	Rabin cipher
نظام رواسب تام	Complete residue system
نظام فيجينير	Vigenere cipher

هـ

هجائية	Alphabet
هجوم تكيفي	Adaptive attack

و

وكالة الأمن القومي	National security agency (NSA)

ي

يقسم	Divide

ثانياً: إنجليزي – عربي

A

Active adversary	عدو فعال (نشط)
Adaptive attack	هجوم تكيفي
Advanced encryption standard (AES)	نظام التعمية القياسي المتقدم
Adversary (Eve)	العدو (حواء)
Algorithms	الخوارزميات
Alphabet	هجائية
Authentication	موثوقية (تطابق الهوية)
Axhaustive keyspace	استنفاد فضاء المفاتيح

B

Baby-step	الخطوة الصغيرة
Bernoulli trials	محاولات بيرنولي
Big-oh notation	رمز O الكبيرة
Block ciphers	أنظمة تعمية قالبية
Block length	طول القالب

C

Ceasar cipher	نظام القيصر
Certificate	شهادة
Certification authority	سلطة الشهادات
Chinese remainder theorem	مبرهنة الباقي الصينية
Chosen-ciphertext	اختيار نص معمى

اختيار نص واضح	Chosen-plaintext
معرفة النص المعمى فقط	Cipher text-only
تعمية سلسلة قوالب	Cipher-block chaning
النص المعمى	Ciphertext
تعمية تقليدية	Classical cryptography
قناة اتصال	Communication channel
نظام رواسب تام	Complete residue system
تعقد الحسابات	Complexity
عدد مؤلف	Composite number
آمن حسابياً	Computationally secure
مسألة حساب Φ	COMPUTE Φ
ضم (تسلسل)	Concatenation
المحافظة على السر	Confidentiality
تشويش	Confusion
فصل تطابق	Congruence class
نظام تطابقات	Congruence system
تحليل التعمية	Cryptanalysis
دالة تمويه تعموية	Cryptographic hash function
برتوكولات تعموية	Cryptographic protocols
علم التعمية	Cryptology

D

ضغط البيانات	Data compression

Date encryption standard (DES)	نظام تعمية البيانات القياسي
Date integrity	سلامة البيانات
Decryption function	دالة كشف المعمى
DHP	مسألة ديفي وهيلمان
Diffusion	النشر
Digital signature	توقيع إلكتروني
Digital signature with appendix	توقيع إلكتروني مع ملحق
Discrete logarithms	اللوغاريتمات المنفصلة
Divide	يقسم
Division algorithm	خوارزمية القسمة
DLP	مسألة اللوغاريتم المنفصل

E

Efficient algorithm	خوارزمية فعالة
Electronic cod book	كتاب التعمية الإلكتروني
ELGAMAL	مسألة الجمل
ELGamal	نظام الجمل
ELGamal signature	توقيع الجمل
Encryption function	دالة التعمية
Encryption schemes	خطط التعمية
Entropy	انتروبيا
Equivalence class	فصل تكافؤ
Euclidean algorithm	خوارزمية إقليدس

دالة أويلر	Euler function
شاهد أويلر	Euler witness
معيار أويلر	Euler's criterion
مبرهنة أويلر	Euler's theorem
عملية الفصل المتنافية (XOR)	Exclusive or (XOR)
تزوير وجودي	Existential forgery
خوارزمية إقليدس الموسعة	Extended Euclidean algorithm

F

مسألة تحليل الأعداد الصحيحة	FACTOR
تحليل الأعداد	Factoring of numbers
نظام تعمية فيستل	Feistel cipher
سلم فيستل ملتو	Feistel twisted ladder
شاهد فيرما	Fermat witness
مبرهنة فيرما الصغرى	Fermat's little theorem
تزوير الرسالة	Forgery
تحليل التردد	Frequency analysis

G

خوارزمية جاوس	Gauss algorithm
مولِّد	Generator
الخطوة الكبيرة	Giant-step
القاسم المشترك الأكبر	Greatest common divisor
زمرة	Group

H

Hash function	دالة تمويه

I

Identification	مطابقة الهوية الشخصية
Impersonation	انتحال الشخصية
In pairs	مثنى مثنى
Index calculus	حساب الدليل
Index of coincidence	معامل الصدفة
Initial seed	بذرة بدائية
Invertible	قابل للعكس

J

Jacobi symbol	رمز جاكوبي

K

Kasiski test	اختبار كاسيكي
Key generating	توليد مفتاح
Key space	فضاء المفاتيح
Known-plaintext	معرفة النص الواضح

L

Least common multiple	المضاعف المشترك الأصغر
Legendre symbol	رمز ليجندر
Linear combination	تركيب خطي
Low of quadratic reciprocity	قانون المقلوب التربيعي

M

طريقة الالتقاء بالمنتصف	Meet-in-the-middle attack
مطابقة هوية الرسالة	Message authentication
شفرة توثيق الرسالة	Message authentication code
شفرة مطابقة هوية الرسالة	Message authentication code
رسالة ملخصة	Message digest
فضاء الرسائل	Message space
اختبار ميلر ورابن	Miller-Rabin test
أشكال العمليات	Modes of operations
شفرة اكتشاف معدلة	Modification detection code
حساب التطابقات	Moduler arithmetic
نظام أحادي	Monoalphabetic cipher
التعمية المتكررة	Multiple encryption
معكوس (نظير) ضربي	Multiplicative inverse

N

وكالة الأمن القومي	National security agency (NSA)
نظام البيانات الجديد المحكم	New data seal (NDS)
عدم الإنكار (التنصل)	Nonrepudiation
منع التزوير	Non-repudiation
قناة غير آمنة	Nonsecure channel
حواشي	Notes
مرشح الحقل العددي	Number field sieve

O

One-time pad	لفافة لمرة واحدة
One-way function	دالة ذات اتجاه واحد
Order of integer	رتبة عدد صحيح

P

Passive adversary	عدو غير فعال
Password	كلمة سر
Plaintext	النص الواضح
Pollard's rho method	طريقة رو لبولارد
Polyalphabetic cipher	نظام تعددي
Polynomial time algorithm	خوارزمية حدودية
Pretty awful privacy	خصوصية سيئة جداً
Pretty good privacy (PGP)	خصوصية جيدة وبارعة
Primality testing	اختبار الأوليات
Prime number	عدد أولي
Prime number theorem	مبرهنة الأعداد الأولية
Provable security	الأمن القابل للبرهان
Provably secure	آمن برهاناً
Pseudosquares	أشباه المربعات
Public-key cryptography	نظام تعمية ذو مفتاح معلن

Q

QRP	مسألة الرواسب التربيعية

الرواسب غير التربيعية	Quadratic nonresidues
الرواسب التربيعية	Quadratic residues
المرشح التربيعي	Quadratic sieve

R

مسألة رابن	RABIN
نظام رابن	Rabin cipher
اختيار عشوائي	Random choice
مربعات عشوائية	Random squares
قيمة عشوائية	Random value
المستقبل (بوب)	Receiver (Bob)
أوليان نسبياً	Relatively prime
شكل رو	Rho-diagram
حلقة	Ring
نظام RSA	RSA cipher
خطة توقيع نظام RSA	RSA Signature scheme

S

تذيل (تمليح) الرسالة	Salting the message
كلمة سر (مفتاح)	Secret word (key)
قناة آمنة	Secure channel
خوارزمية التموية الآمنة	Secure hash
المرسل (أليس)	Sender (Alice)
برتوكول الثلاث خطوات لشامير	Shamir's 3-pass protocol

Shift cipher	نظام الازاحة
Simple substitution cipher	نظام تعويض بسيط
Smartcard	بطاقة ذكية
Solovay-Strassen test	اختبار سولوفي وستراسن
SQROOT	مسألة الجذور التربيعية
Square and multiply algorithm	خوارزمية التربيع والضرب
Square roots	جذور تربيعية
State ciphers	أنظمة المرحلة
Stream ciphers	أنظمة السيل
Strong witness	شاهد قوي
Subliminal channel	قناة مخفية
Symmetric-key encryption	التعمية ذات المفتاح المتماثل
Symmetric-key schemes	خطط المفتاح المتماثل

T

The integers	الأعداد الصحيحة
The integers odulo n	الأعداد الصحيحة قياس n
Trapdoor function	دالة ذات باب سري

U

Unconditionally secure	آمن تماماً
Universal exponent	قوة شاملة

V

VENONA	تعمية فينونا

نظام تعمية فيرنام	Vernam cipher
نظام فيجينير	Vigenere cipher

Z

عدم المعرفة مطلقاً	Zero-knowledge

كشاف الموضوعات
index

أ

ج

ح

خ

ص

ض

ط